Effective January 20, 2026. This Data Processing Agreement supersedes and replaces all prior versions.

# 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 Order (sometimes referred to as "you," or "your,") and, together with the Order, Master Services Agreement, Schedule of Services, and other relevant Service Attachments, 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 HIPAA is identified in the Order, and 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.

**Definitions**. For purposes of this Business Associate Agreement ("BAA"), the Parties give the following meaning to each of the terms. Any capitalized term used in this BAA, but not otherwise defined, has the meaning given to that term in the Privacy Rule or pertinent law.

**A.** "Affiliate" means a subsidiary or affiliate of Covered Entity that is, or has been, considered a covered entity, as defined by HIPAA.

**B.** "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI, as defined in 45 CFR §164.402.

**C.** "Breach Notification Rule" means the portion of HIPAA set forth in Subpart D of 45 CFR Part 164.

**D.** "Data Aggregation" means, with respect to PHI created or received by Business Associate in its capacity as the "business associate" under HIPAA of Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate in its capacity as a business associate of one or more other "covered entity" under HIPAA, to permit data analyses that relate to the Health Care Operations (defined below) of the respective covered entities. The meaning of "data aggregation" in this BAA shall be consistent with the meaning given to that term in the Privacy Rule.

**E.** "Designated Record Set" has the meaning given to such term under the Privacy Rule, including 45 CFR §164.501.B.

**F.** "De-Identify" means to alter the PHI such that the resulting information meets the

requirements described in 45 CFR §§164.514(a) and (b).

**G.** "Electronic PHI" means any PHI maintained in or transmitted by electronic media as defined in 45 CFR §160.103.

**H.** "Health Care Operations" has the meaning given to that term in 45 CFR §164.501.

**I.** "HHS**"** means the U.S. Department of Health and Human Services.

**J.** "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.

**K.** "Individual" has the same meaning given to that term i in 45 CFR §§164.501 and 160.130 and includes a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

**L.** "Privacy Rule" means that portion of HIPAA set forth in 45 CFR Part 160 and Part 164, Subparts A and E.

**M.** "Protected Health Information" or "PHI" has the meaning given to the term "protected health information" in 45 CFR §§164.501 and 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

**N.** "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**O.** "Security Rule" means the Security Standards for the Protection of Electronic Health Information provided in 45 CFR Part 160 & Part 164, Subparts A and C.

**P.** "Unsecured Protected Health Information" or "Unsecured PHI" means any "protected health information" as defined in 45 CFR §§164.501 and 160.103 that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary in the guidance issued pursuant to the HITECH Act and codified at 42 USC §17932(h).

**Use and Disclosure of PHI.**

**A.** Except as otherwise provided in this BAA, Business Associate may use or disclose PHI as reasonably necessary to provide the services described in the Agreement to Covered Entity, and to undertake other activities of Business Associate permitted or required of Business Associate by this BAA or as required by law.

**B.** Except as otherwise limited by this BAA or federal or state law, Covered Entity authorizes Business Associate to use the PHI in its possession for the proper management and administration of Business Associate's business and to carry out its legal responsibilities. Business Associate may disclose PHI for its proper management and administration, provided that (i) the disclosures are required by law; or (ii) Business Associate obtains, in writing, prior to making any disclosure to a third party (a) reasonable assurances from this third party that the PHI will be held confidential as provided under this BAA and used or further disclosed only as required by law or for the purpose for which it was disclosed to this third party and (b) an agreement from this third party to notify Business Associate immediately of any breaches of the confidentiality of the PHI, to the extent it has knowledge of the breach.

© Scott & Scott, LLP

**C.** Business Associate will not use or disclose PHI in a manner other than as provided in this BAA, as permitted under the Privacy Rule, or as required by law. Business Associate will use or disclose PHI, to the extent practicable, as a limited data set or limited to the minimum necessary amount of PHI to carry out the intended purpose of the use or disclosure, in accordance with Section 13405(b) of the HITECH Act (codified at 42 USC §17935(b)) and any of the act's implementing regulations adopted by HHS, for each use or disclosure of PHI.

**D.** Upon request, Business Associate will make available to Covered Entity any of Covered Entity's PHI that Business Associate or any of its agents or subcontractors have in their possession.

**E.** Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

**Safeguards Against Misuse of PHI**. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided by the Agreement or this BAA and Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate agrees to take reasonable steps, including providing adequate training to its employees to ensure compliance with this BAA and to ensure that the actions or omissions of its employees or agents do not cause Business Associate to breach the terms of this BAA.

**Reporting Disclosures of PHI and Security Incidents**. Business Associate will report to Covered Entity in writing any use or disclosure of PHI not provided for by this BAA of which it becomes aware and Business Associate agrees to report to Covered Entity any Security Incident affecting Electronic PHI of Covered Entity of which it becomes aware. Business Associate agrees to report any such event within five business days of becoming aware of the event.

**Reporting Breaches of Unsecured PHI**. Business Associate will notify Covered Entity in writing promptly upon the discovery of any Breach of Unsecured PHI in accordance with the requirements set forth in 45 CFR §164.410, but in no case later than 30 calendar days after discovery of a Breach. Business Associate will reimburse Covered Entity for any costs incurred by it in complying with the requirements of Subpart D of 45 CFR §164 that are imposed on Covered Entity as a result of a Breach committed by Business Associate.

**Mitigation of Disclosures of PHI**. Business Associate will take reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of any use or disclosure of PHI by Business Associate or its agents or subcontractors in violation of the requirements of this BAA.

**Agreements with Agents or Subcontractors**. Business Associate will ensure that any of its agents or subcontractors that have access to, or to which Business Associate provides, PHI agree in writing to the restrictions and conditions concerning uses and disclosures of PHI contained in this BAA and agree to implement reasonable and appropriate safeguards to protect any Electronic PHI that it creates, receives, maintains or transmits on behalf of Business Associate or, through the Business Associate, Covered Entity. Business Associate shall notify Covered Entity, or upstream Business Associate, of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract by placement of such notice on the Business Associate's primary website. Business Associate shall ensure that all subcontracts and agreements provide the same level of privacy and security as this BAA.

**Audit Report.** Upon request, Business Associate will provide Covered Entity, or upstream Business Associate, with a copy of its most recent independent HIPAA compliance report (AT-C 315), HITRUST certification or other mutually agreed upon independent standards based third party audit report. Covered entity agrees not to re-disclose Business Associate's audit report.

© Scott & Scott, LLP

**Access to PHI by Individuals**.

**A.** Upon request, Business Associate agrees to furnish Covered Entity with copies of the PHI maintained by Business Associate in a Designated Record Set in the time and manner designated by Covered Entity to enable Covered Entity to respond to an Individual's request for access to PHI under 45 CFR §164.524.

**B.** In the event any Individual or personal representative requests access to the Individual's PHI directly from Business Associate, Business Associate within ten business days, will forward that request to Covered Entity. Any disclosure of, or decision not to disclose, the PHI requested by an Individual or a personal representative and compliance with the requirements applicable to an Individual's right to obtain access to PHI shall be the sole responsibility of Covered Entity.

**Amendment of PHI**.

**A.** Upon request and instruction from Covered Entity, Business Associate will amend PHI or a record about an Individual in a Designated Record Set that is maintained by, or otherwise within the possession of, Business Associate as directed by Covered Entity in accordance with procedures established by 45 CFR §164.526. Any request by Covered Entity to amend such information will be completed by Business Associate within 15 business days of Covered Entity's request.

**B.** In the event that any Individual requests that Business Associate amend such Individual's PHI or record in a Designated Record Set, Business Associate within ten business days will forward this request to Covered Entity. Any amendment of, or decision not to amend, the PHI or record as requested by an Individual and compliance with the requirements applicable to an Individual's right to request an amendment of PHI will be the sole responsibility of Covered Entity.

**Accounting of Disclosures**.

**A.** Business Associate will document any disclosures of PHI made by it to account for such disclosures as required by 45 CFR §164.528(a). Business Associate also will make available information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosures in accordance with 45 CFR §164.528. At a minimum, Business Associate will furnish Covered Entity the following with respect to any covered disclosures by Business Associate: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI, and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure which includes the basis for such disclosure.

**B.** Business Associate will furnish to Covered Entity information collected in accordance with this Section 10, within ten business days after written request by Covered Entity, to permit Covered Entity to make an accounting of disclosures as required by 45 CFR §164.528, or in the event that Covered Entity elects to provide an Individual with a list of its business associates, Business Associate will provide an accounting of its disclosures of PHI upon request of the Individual, if and to the extent that such accounting is required under the HITECH Act or under HHS regulations adopted in connection with the HITECH Act.

**C.** In the event an Individual delivers the initial request for an accounting directly to Business Associate, Business Associate will within ten business days forward such request to Covered Entity.

**Availability of Books and Records**. Business Associate will make available its internal practices, books, agreements, records, and policies and procedures relating to the use and disclosure of PHI, upon request, to the Secretary of HHS for purposes of determining Covered Entity's and Business Associate's compliance with HIPAA, and this BAA.

© Scott & Scott, LLP

**Responsibilities of Covered Entity**. With regard to the use and/or disclosure of Protected Health Information by Business Associate, Covered Entity agrees to:

**A.** Notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

**B.** Notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

**C.** Notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

**D.** Except for data aggregation or management and administrative activities of Business Associate, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

**Data Ownership.** Business Associate's data stewardship does not confer data ownership rights on Business Associate with respect to any data shared with it under the Agreement, including any and all forms thereof.

**Effect of BAA**.

**A.** This BAA is a part of and subject to the terms of the Agreement, except that to the extent any terms of this BAA conflict with any term of the Agreement, the terms of this BAA will govern.

**B.** Except as expressly stated in this BAA or as provided by law, this BAA will not create any rights in favor of any third party.

**Regulatory References**. A reference in this BAA to a section in HIPAA means the section as in effect or as amended at the time.

**Amendments and Waiver**. This BAA may not be modified, nor will any provision be waived or amended, except in writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

**HITECH Act Compliance**. The Parties acknowledge that the HITECH Act includes significant changes to the Privacy Rule and the Security Rule. The privacy subtitle of the HITECH Act sets forth provisions that significantly change the requirements for business associates and the agreements between business associates and covered entities under HIPAA and these changes may be further clarified in forthcoming regulations and guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued with respect to the HITECH Act. The Parties also agree to negotiate in good faith to modify this BAA as reasonably necessary to comply with the HITECH Act and its regulations as they become effective but, in the event that the Parties are unable to reach agreement on such a modification, either Party will have the right to terminate this BAA upon 30- days' prior written notice to the other Party.

**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"). If GLBA is identified in the Order, and if Provider's services constitute processing of financial information governed by GLBA, these provisions shall apply.

**a. DEFINITIONS**

© Scott & Scott, LLP

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. Department of Defense Standards for Controlled Unclassified Information ("CUI").** This section documents the safeguards imposed to protect CUI subject to the DoD and CMMC's standards. If CUI or CMMC are identified in the Order, and to the extent Provider's services involve CUI subject to DoD or CMMC standards or regulations, these provisions shall apply.

**a. System Environment.** Provider will prepare a detailed description of system boundaries, system interconnectedness, and key devices.

**b. Requirements.** Provider will thoroughly describe how the CMMC requirements have been implemented for each of the following:

**i.** Access Control
**ii.** Awareness and Training
**iii.** Audit and Accountability

© Scott & Scott, LLP

iv. Configuration Management
v. Identification and Authentication
vi. Incident Response
vii. Maintenance
viii. Media Protection
ix. Personnel Security
x. Physical Protection
xi. Risk Assessment
xii. Security Assessment
xiii. System and Communication Protection
xiv. System and Information Integrity

c. **Definitions.** As used in this section —

Compromise means disclosure of information to unauthorized persons, for a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Covered defense information means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Other Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

d. **Restrictions**. Provider agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber

© Scott & Scott, LLP

incident pursuant to DFARS clause252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) Provider shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) Provider shall protect the information against unauthorized release or disclosure.

(3) Provider shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject Provider to—

- Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and
- Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third-party beneficiary of this clause.

**e.** Subcontracts. The Contractor shall include this clause, including this paragraph(c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial products and commercial services, without alteration, except to identify the parties.

**4. 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"). If CCPA is identified in the Order, and 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.

© Scott & Scott, LLP

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.

f. **Data Retention.** Provider will retain only the minimum amount of data that is essential to fulfill its obligations under the Master Services Agreement, Service Attachments, and this DPA. Provider will not keep data longer than is necessary without first providing notice to the Client with a justification of the extended retention.

5. **Colorado Privacy Act.** This section documents the safeguard standards imposed to protect Client information subject to the Colorado Privacy Act (6-1-1301) ("CPA"). If CPA is identified in the Order, and to the extent Provider's services constitute processing of personal information governed by CPA, these provisions shall apply.

Provider shall adhere to the instructions of the controller and assist the controller to meet its obligations under the CPA.

Taking into account the nature of processing and the information available to Provider, Provider shall assist the controller by:

a. taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the controller's obligation to respond to consumer requests to exercise their rights pursuant to section 6-1-1306;

b. helping to meet the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of the security of the system pursuant to section 6-1-716; and

c. providing information to the controller necessary to enable the controller to conduct and document any data protection assessments required by section 6-1-1309.

Notwithstanding the instructions of the controller, Provider shall:

a. ensure that each person processing the personal data is subject to a duty of confidentiality with respect to the data; and
b. engage a subcontractor only after providing the controller with an opportunity to object and pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

Taking into account the context of processing, Provider shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between Provider and the controller to implement the measures.

© Scott & Scott, LLP

Processing by Provider must be governed by a contract between the controller and Provider that is binding on both parties and that sets out:

a. the processing instructions to which the processor is bound, including the nature and purpose of the processing;
b. the type of personal data subject to the processing, and the duration of the processing; and
c. the following requirements:
    (i) at the choice of the controller, Provider shall delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

(ii) (a) Provider shall make available to the controller all information necessary to demonstrate compliance with the obligations; and

(b) Provider shall allow for, and contribute to, reasonable audits and inspections by the controller or the controller's designated auditor. Alternatively, Provider may, with the controller's consent, arrange for a qualified and independent auditor to conduct, at least annually and at Provider's expense, an audit of the Provider's policies and technical and organizational measures in support of its obligations under the CPA using an appropriate and accepted control standard or framework and audit procedure for the audits as applicable. Provider shall furnish a report of the audit to the controller upon request.

6. **Connecticut Privacy Act.** This section documents the safeguard standards imposed to protect Client information subject to the Connecticut SB 12-2 ("Conn Act"). If Conn Act is identified in the Order, and to the extent Provider's services constitute processing of personal information governed by Conn Act, these provisions shall apply.

Provider shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under the Conn Act. Such assistance shall include:

a. taking into account the nature of processing and the information available to Provider, providing appropriate technical and organizational measures to fulfill the controller's obligation to respond to consumer rights requests;

b. taking into account the nature of processing and the information available to Provider, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security of Provider's systems, in order to meet the controller's obligations; and

c. providing necessary information to enable the controller to conduct and document data protection assessments.

Provider shall have a written contract with the controller that will govern the Provider's data-processing procedures with respect to processing performed on behalf of the controller. The contract shall be binding and clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract shall also require that Provider:

a. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

b. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

© Scott & Scott, LLP

c. Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate Provider's compliance with the obligations

d. after providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of Provider with respect to the personal data; and

e. allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of Provider's policies and technical and organizational measures in support of the obligations of the Conn Act using an appropriate and accepted control standard or framework and assessment procedure for such assessments.

Provider shall provide a report of such assessment to the controller upon request.

For purposes of the Conn Act, the following definitions apply:

a. "Consumer" means an individual who is a resident of this state. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit or government agency whose communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit or government agency.

b. "Controller" means an individual who, or legal entity that, alone or jointly with others determines the purpose and means of processing personal data.

c. "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable individual. "Personal data" does not include de-identified data or publicly available information.

d. "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

e. "Processor" means an individual who, or legal entity that, processes personal data on behalf of a controller

**7. 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. If SHIELD is identified in the Order and to the extent Provider's services constitute processing of data under SHIELD, these provisions will apply. The Data Processing Agreement 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;

© Scott & Scott, LLP

- 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

© Scott & Scott, LLP

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

© Scott & Scott, LLP

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.

8. **Virginia Privacy Act.** This section documents the safeguard standards imposed to protect Client information subject to the Code of Virginia Section 59.1-579 ("VPA"). If VPA is identified in the Order, and to the extent Provider's services constitute processing of personal information governed by VPA, these provisions shall apply:

.

**a.** This DPA sets forth instructions for the following:
    **i.** Provider may provide hosting services and will only process data that is deposited by Client into Provider's systems;
    **ii.** Provider will not use non-anonymized protected data for any of its own business purposes;
    **iii.** Any processing will be for a reasonable amount of time given the Services to be performed; and
    **iv.** Both Provider and Client have the right to adjust whether Client may deposit protected data into Provider's systems.

**b.** With respect to the protected data, Provider shall:
    **i.** Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
    **ii.** At the Client's direction, delete or return all protected data to the Client as requested at the end of the provision of services, unless retention of the protected data is required by law;
    **iii.** Upon the reasonable request of the Client, make available to the Client all information in its possession necessary to demonstrate the Provider's compliance with the obligations in this chapter;
    **iv.** Allow, and cooperate with, reasonable assessments by the Client the Client's designated assessor; alternatively, Provider may arrange for a qualified and independent assessor to conduct an assessment of the Provider's policies and technical and organizational measures in support of the obligations under this chapter using an appropriate and accepted control standard or framework and assessment procedure for such assessments. Provider shall provide a report of such assessment to the Client upon request; and

© Scott & Scott, LLP

**v.** Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the Provider with respect to the protected data.

## 9. General Data Protection Regulation for the EU and UK ("GDPR")

The General Data Protection Regulation ("GDPR") for the EU and UK 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 GDPR is identified in the Order, and to the extent Provider's services constitute processing of personal information governed by GDPR, these provisions shall apply

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 date of the Order ("Addendum Effective Date").

**DEFINITIONS**

"GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation and the UK Data Protection Act of 2018 (collectively "GDPR"), 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.

© Scott & Scott, LLP

(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 presented 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

© Scott & Scott, LLP

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.

**ANNEX TO STANDARD CONTRACTUAL CLAUSES**

© Scott & Scott, LLP

*Purpose and scope*

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Effect and invariability of the Clauses*

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Third-party beneficiaries*

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

© Scott & Scott, LLP

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Interpretation*

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Hierarchy*

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, the Order controls, followed by the DPA and then the MSA.

*Description of the transfer(s)*

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

## OBLIGATIONS OF THE PARTIES

*Data protection safeguards*

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

*Instructions*

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations

© Scott & Scott, LLP

on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

*Purpose limitation*

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

*Transparency*

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

*Accuracy*

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

*Duration of processing and erasure or return of data*

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

*Security of processing*

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information

© Scott & Scott, LLP

for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It 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) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

*Sensitive data*

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in this Annex.

*Onward transfers*

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union market to the three EEA States Iceland, Liechtenstein and Norway. The Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

© Scott & Scott, LLP

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

*Documentation and compliance*

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Use of sub-processors*

(a) GENERAL WRITTEN AUTHORISATION. The data importer has the controller's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that

© Scott & Scott, LLP

provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

*Data subject rights*

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorized to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

*Redress*

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her

© Scott & Scott, LLP

habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Liability*

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party(ies) by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Supervision*

(a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the

© Scott & Scott, LLP

(c) competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

*Local laws and practices affecting compliance with the Clauses*

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards; any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has

© Scott & Scott, LLP

reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

***Obligations of the data importer in case of access by public authorities***

*Notification*

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer to inform the data exporter promptly where it is unable to comply with these Clauses.

*Review of legality and data minimization*

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that

© Scott & Scott, LLP

there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer.

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## FINAL PROVISIONS

*Non-compliance with the Clauses and termination*

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated.

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

© Scott & Scott, LLP

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Governing law*

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 United States.

*Choice of forum and jurisdiction*

Any dispute arising from these Clauses shall be resolved by the courts of the United States.

**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

© Scott & Scott, LLP

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.

© Scott & Scott, LLP