Data Processing Addendum

Last updated September 11, 2023

This **DATA PROCESSING ADDENDUM** ("**DPA**") is made and entered into by and between Simeio Solutions, LLC or its Affiliate (as defined below) entering into this DPA (hereinafter, the "**Company**") and the Company's Vendor also entering into this DPA ("**Vendor**"), as a supplement to an underlying business agreement between the parties.

1. **Definitions**. All capitalized terms have the meanings as set forth in this Addendum, or if not defined, then as set forth within Regulation (EU) 2016/679 of the European Parliament (the General Data Protection Regulation or "**GDPR**"), or if not defined within the GDPR, then as defined within the United Kingdom General Data Protection Regulation ("**UK GDPR**"), or if not defined within the UK GDPR, then as defined within the California Consumer Privacy Act of 2018 ("**CCPA**") as amended by the California Privacy Rights Act of 2020 ("**CPRA**"), or if not defined within either the GDPR, the UK GDPR, the CCPA, or the CPRA, then as defined within the underlying Agreement.
    a. "**Affiliate**" means any company or entity that is under common control with, a subsidiary of, or a parent company to Company.
    b. "**Agreement**" means the underlying business agreement between the parties, pursuant to which data will be processed that is subject to the CCPA, CPRA, GDPR or UK GDPR.
    c. "**CCPA**" means the California Consumer Protection Act, Cal. Civ. Code § 1798.100 *et seq*., and its implementing regulations.
    d. "**CPRA**" means the California Privacy Rights Act of 2020 (2020 Cal. Legis. Serv. Proposition 24, codified at Cal. Civ. Code §§ 1709.100, et seq.) and its implementing regulations, as amended or superseded from time to time.
    e. "**Simeio Personal Information**" means any data, file attachment, text, images, reports, or other information that is transferred between the parties for Services pursuant to the Agreement and that directly or indirectly identifies or relates to a Data Subject.
    f. "**Contracted Processor**" means the Processor or a Subprocessor, that will be processing the data pursuant to the Agreement.
    g. "**Data Protection Laws**" means the CCPA and CPRA to the extent Client Personal Information includes that of California residents pursuant to the Agreement, the GDPR to the extent Client Personal Information includes that of EEA residents pursuant to the Agreement, the UK GDPR to the extent Client Personal Information includes that of UK residents pursuant to the Agreement and, to the extent applicable, the data protection or privacy laws of any other state province, or country.
    h. "**Data Subject**" means (i) an identified or identifiable natural person who is in the EEA or whose rights are protected by the GDPR; and (ii) a "Consumer" as the term is defined in the CCPA and CPRA.
    i. "**DPA**" means this Data Protection Addendum.
    j. "**EEA**" means the European Economic Area and includes all countries with the EU in addition to Iceland, Liechtenstein and Norway.
    k. "**EU**" means the European Union.

l. "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of June 4, 2021.

m. "**Services**" has the definition set forth in the Agreement and includes the processing of Client Personal Information pursuant to the Agreement or any applicable Statement of Work ("**SOW**").

n. "**UK**" means the United Kingdom of Great Britain and Northern Ireland.

2. This DPA supplements the existing Agreement between the parties and except as supplemented by this DPA, the terms of the Agreement will remain in full force and effect.

3. Each party agrees to comply with their respective obligations under applicable Data Protection Laws.
4. The parties agree to avoid taking any action that would cause the other party to be deemed to have sold Client Personal Information under the CCPA or CPRA. In no event will the transfer of Client Personal Information, pursuant to the Agreement, result in or be construed as constituting a sale of such Client Personal Information by or to Company.
5. In regard to the transfer of data for data processing occurring pursuant to the Agreement, the parties agree to be bound by the SCCs, applying the following Module:
    a. If the transfer of data for data processing pursuant to the Agreement is from Controller to Controller, then Module One of the SCCs will apply;
    b. If the transfer of data for data processing pursuant to the Agreement is from Controller to Processor, then Module Two of the SCCs will apply;
    c. If the transfer of data for data processing pursuant to the Agreement is from Processor to Processor, then Module Three of the SCCs will apply; or
    d. If the transfer of data for data processing pursuant to the Agreement is from Processor to a Controller not otherwise subject to the GDPR, then Module Four or the SCCs will apply;

    A current copy of the SCCs is located at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914 and the specific SCCs applicable to this DPA are hereby incorporated into this DPA by reference as if fully restated herein.
6. For purposes of selecting optional (or otherwise selectable) language in the SCCs:
    a. Clause 7 will not apply.
    b. For Clause 9(a), Option 2 (general written authorization for sub-processors) will apply with the specified time period being thirty (30) calendar days.
    c. For Clause 11(a), the optional language (data subject's ability to lodge complaint with an independent resolution body) will not apply.
    d. For Clause 17, Option 1 will apply, the parties agree that the choice of law governing this DPA will be the law of Ireland.
    e. For Clause 18, the parties agree that any dispute arising from this DPA will be resolved in the courts of Ireland.
    f. If the Client Personal Information is governed by the UK GDPR, this DPA will include the Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on February 2, 2022, as it is revised under Section 18 of those Mandatory Clauses.

7. For the purposes of **Annex I.A.** to the SCCs, the identity and contact details of the parties are as set forth within the introductory paragraph or signature page(s) of the underlying Agreement and, where applicable, their data protection officer(s) and/or representative(s) in the European Union are specified within the applicable SOW.
8. For purposes of **Annex I.B.** to the SCCs, if Client Personal Information is being processed pursuant to the Services, the applicable SOW will specify the nature of the data processing, categories of data subjects whose data is to be transferred, categories of personal data transferred, whether sensitive data will be transferred and a description of such sensitive data, frequency of the transfer, purpose of the data transfer and further processing, the period for which the Client Personal Information will be retained, and if the transfer will involve use of sub-processors, the subject matter, nature and duration of the sub-processing.
9. For purposes of **Annex I.C.,** to the SCCs, if Client Personal Information is being processed pursuant to the Services, the applicable SOW will specify the applicable supervisory authority, unless such processing is governed by the UK GDPR.
10. For purposes of **Annex II** to the SCCs, if Client Personal Information is being processed pursuant to the Services, unless the SOW specifies different technical and organizational measures, the following minimum technical and organizational measures will be implemented by the data importing partyc:
    a. Physical Access Controls
        - Locked doors on all entrances and exits including electronic key card access on all data processing and data center facilities.
        - Removal of data and data center access upon personnel termination or change to a new role that does not require access to fulfill obligations under the Agreement.
        - Conduct periodic access reviews and audits.
        - Video monitoring of premises, including entrances and exits via CCTV.
        - Security breach alarms.
    b. Systems Access Control
        - Unique usernames for each user or personnel.
        - No sharing of accounts or identities.
        - Utilization of strong/complex passwords with minimum length requirements.
        - Utilization of multi-factor authentication for remote access.
        - Password expiration at regular intervals.
        - Forced password reset at first login.
        - Maximum failed login attempts with account lockout.
        - Strong protection for password repositories or databases, such as encryption.
        - Encryption of authentication information in transit.
        - Timeout sessions due to user inactivity.
    c. Access Control
        - Approval from appropriate management personnel is required for individual access to information and systems.
        - Removal of individual access upon termination or change to a new role that does not require access to fulfill obligations under the Agreement.
        - Logging and monitoring of failed attempts to access personal data.

- Encryption at rest for personal data, including data resting on all portable media such as laptops, backup devices and USB drives.
- Access control where applicable to prevent inappropriate data use.
- Employee background checks and confidentiality agreements.

d. Transmission Control
- Restrictions of transfer rights for systems containing personal data.
- Utilization of secure data transit networks such as VPN, SFTP, SSL, and email encryption.

e. Input Control (logging monitoring and auditing)
- Logging of input actions in systems containing personal data.
- Logging of failed attempts to edit, delete or change personal data.
- Auditing of actions to ensure consistency with above requirements.

f. Availability Control
- Written policies implementing information security controls such as firewalls, anti-virus software, application controls, IPS/IDS, monitoring & alerting, segmented networks, vulnerability management, patch management, and hardened system standards.
- Documented disaster recovery and business continuity protocols.
- Secure backup procedures in place with full backup availability. Including at backup facilities with security features that include:
  - Environmental controls.
  - Fire protection.
  - Uninterruptible power supply.
  - Physical security.

g. Separation Control
- Logical separation of data between production, QA and development networks.
- Separation of duties and access for personnel processing relevant personal data and personnel not processing relevant personal data.

11. For purposes of **Annex III** to the SCCs, if Client Personal Information is being processed pursuant to the Services, the applicable SOW will identify any sub-processors that are anticipated and describe the processing of Client Personal Data that will be handled by such sub-processors.
12. Information provided herein or within an applicable SOW to satisfy Annexes I, II and III to the SCCs is included as may be required by the Data Protection Laws. Nothing in Sections 8, 9, 10, and 12 of this DPA confers any right or imposes any obligation on a party to this DPA.
13. The parties agree to cooperate fully with each other regarding compliance obligations pursuant to this DPA. Such cooperation will include providing information relevant to conduct necessary audits or assessments and fulfillment of Data Subject requests including, but not limited to, access, erasure, opt-out and objection.
14. General Terms. This DPA constitutes the entire agreement between the parties relating to the processing of personal data and supersedes any prior agreements between the parties relating to the subject matter of this DPA. To the extent of any conflict between the terms of this DPA and the terms of the Agreement with respect to the subject matter of this DPA and solely where Data Protection Laws apply, the terms of this DPA will control. This DPA may only amended if in writing and signed by the parties to this agreement. The provisions of this DPA are severable. If any provision is determined to be invalid, illegal, or unenforceable, in

whole or in part, the remaining provisions and any partially enforceable provisions will remain in full force and effect. For avoidance of doubt, as between the parties to this DPA, each party's liability and remedies under this DPA are subject to the liability limitations and damages exclusions set forth in the Agreement. Notwithstanding the foregoing, Company's total liability will not exceed its insurance policy limits in the aggregate.