TEMPLUM®

GLOBAL DATA PROTECTION ADDENDUM

In connection with that certain User Agreement between Templum, Inc. ("**Templum**" or "**Service Provider**") and each user ("**Client**") (the "**Agreement**"), Templum may Process Personal Data (each as defined below) for or on behalf of Client. Templum agrees to protect and Process Personal Data only in accordance with the terms and conditions set forth in this Data Protection Addendum (this "**Addendum**").

1. Definitions and Interpretation.

(a) "**Applicable Privacy Law**" means any applicable constitution, law, statute, treaty, rule, regulation, directive, ordinance, order, code, interpretation, judgment, decree, injunction, permit, license, authorization, requirement, practice or decision of or agreement with or by any legislative, judicial, administrative, public, or other governmental. This may include, the California Consumer Privacy Act of 2018 ("**CCPA**"), as amended by California Privacy Rights Act of 2020 ("**CPRA**"), the Gramm-Leach-Bliley Act ("**GLBA**"), the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), and the UK Data Protection Act 2018.

(b) "**Client Personal Information**" shall mean Personal Data (as defined below) provided by or on behalf of Client to Templum in connection with Templum's performance of Services pursuant to the Agreement.

(c) "**Confidential Information**" has the meaning provided in the main body of the Agreement, and includes all information, data and other materials generated or derived from Confidential Information.

(d) "**Party**" means Templum and Client, and "Parties" means Templum and Client, collectively.

(e) "**Personal Data**" means any information or set of information that identifies, relates to, describes, is capable of being associated with, or could be linked, directly or indirectly, with an identified or identifiable natural person ("Data Subject"), as well as any other information defined or treated by Applicable Privacy Law as personal information, and includes all information, data and other materials generated or derived therefrom, including any de-identified or aggregated data. Personal Data does not include de-identified or aggregated data or information.

(f) "**Process**," "**Processing**" or "**Processing**," means any operation or set of operations that is performed upon data or information, or on sets of data or information, whether or not by automated means, including collection, recording, storing, retention, aggregation, alteration, use, disclosure, access, transfer, transmission, or destruction.

(g) "**Services**" has the meaning set forth in the main body of the Agreement, except that, solely for purposes of this Addendum, Services shall not include Third Party Services (as defined in the main body of the Agreement).

(h) "**SCCs**" means the Standard Contractual Clauses set out in Commission Implementing Decision (EU) 2021/914 of June 4, 2021 and as amended from time to time.

(i) "**Sub-Processor**" means any Person (as defined in the main body of the Agreement) that is not an employee, officer or director of Templum that provides any element of the Services or Processes Client Personal Information.

(j) "**UK Addendum**" means the UK International Data Transfer Addendum.

The words "including" or "includes" shall not be limiting, and shall be deemed to state "without limitation". Conjugates of defined terms shall have the meanings assigned to the defined terms. Any capitalized terms used herein but not otherwise defined shall have the meanings provided under Applicable Privacy Law.

2. General.

(a) As between Client and Templum, with respect to the Processing of Personal Data under the Agreement, Client shall be the Controller, and Templum shall be the Processor (as defined under Applicable Privacy Law).

(b) Client confirms that it has the right to supply Client Personal Information to Templum and Client will not breach Applicable Privacy Laws. Client represents that it shall comply with all Applicable Privacy Laws and acknowledges and agrees that, as between the Parties, Client is responsible for providing any required notices to, and/or obtaining any required consents or authorizations from, Data Subjects of the Client Personal Information and/or regulatory authorities, as applicable, in connection with Client Personal Information.

(c) Neither Party will by act or omission put the other in breach of the Applicable Privacy Laws.

(d) Templum will not Process or Transfer (as defined in Article 44 of the GDPR) any Personal Data to any third country or international organization outside the EEA or UK unless (i) subject to an adequacy decision or (ii) where such Transfer is made in compliance with Applicable Privacy Laws, whereby Templum will adopt appropriate safeguards, such as entering SCCs and/or UK Addendum where necessary and carry out a transfer impact assessment as required under Applicable Privacy Laws.

(e) The Parties agree that the SCCs (Module Two – Controller to Processor) and the UK Addendum are incorporated into this Addendum by reference and at all times during the term of the Agreement, Client (as data exporter) and Templum (as data importer) shall comply with the SCCs and UK Addendum with respect to Client Personal Information relating to EU and UK data subjects, as applicable. The Parties hereby acknowledge and agree that each Party's signature to the Agreement shall constitute such Party's signature to the SCCs and/or UK Addendum, as required by Applicable Privacy Laws and to the extent the SCCs apply.

(f) The categories of Data Subjects and types of Client Personal Information anticipated to be provided to Templum in connection with the performance of Services are set forth on the attached Appendix 1 to Data Protection Addendum.

(g) To the extent SCC Module(s) Two and/or Three of the SCCs apply(ies), the Parties hereby

agree that, (1) the data exporter is Client and the data importer is Templum; (2) Clause 7 of the SCCs shall be applicable, enabling third parties to accede to this Addendum at any time provided the Controller and Processor are in written agreement; (3) option 2 of Clause 9 of the SCCs is selected and completed by reference to Section 2(m) of this Addendum; (4) clause 11 of the SCCs does not apply (redress); (5) for Clause 13 for transfers to which the GDPR applies, the supervising authority will be decided in accordance with option 1; (6) the governing law and jurisdiction of the SCCs for Clauses 17 and 18 of the SCCs will be the governing law and jurisdiction of Ireland; (7) Annex 1 of the SCCs is completed by reference to Appendix 1; and (8) Annex 2 of the SCCs is completed by reference to the attached Appendix 2 to Data Protection Addendum.

(h) To the extent the UK Addendum applies, the Parties hereby agree that (1) table 1 - the Parties are as set out in this Agreement and Addendum and no further signature is required; (2) table 2 - the version of the approved SCCs is as set out in this Addendum; (3) table 3 – the information is set out in Appendix 1 to this Addendum; and (4) table 4 – the data importer and the data exporter can end the UK Addendum.

(i) Templum will, to the extent legally permissible, notify Client without undue delay if Templum receives a request from a Data Subject of Client Personal Information seeking to exercise such Data Subject's rights under Applicable Privacy Laws ("**Data Subject Access Request**"), and will, on Client's reasonable request, provide reasonable assistance in connection with Clients's response to such Data Subject Access Request. Further, Templum will implement appropriate technical and organizational measures to assist Client with responding to requests from a Data Subject who wishes to exercise their rights under Applicable Privacy Laws.

(j) Templum shall implement and maintain appropriate administrative, technical, and physical measures that are reasonably designed protect any Client Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access. Templum will notify Client promptly upon becoming aware of any unauthorized disclosure of or access to any Client Personal Information (a "**Security Incident**"). Such notification will be provided within seventy-two (72) hours of Templum's confirmation of such Security Incident, except to the extent that Templum is required by applicable laws to delay notification. Templum will investigate the Security Incident and, to the extent the Security Incident results from Templum's breach of an obligation under the Agreement or Addendum, Templum shall: (i) take reasonable steps to mitigate the effects of, and to minimize any damage resulting from, such Security Incident; and (ii) promptly make available to Client information describing the root cause and scope of the Security Incident as well as Templum's proposed remediation steps. Further, if required, Templum will assist Client as reasonably required to notify any relevant data protection Supervisory Authority of any Security Incident.

(k) Templum will assist Client with its obligations under Applicable Privacy Laws as reasonably required, including assisting Client with a privacy impact assessment.

(l) Templum shall ensure that Templum's personnel authorized by Templum to process Client Personal Information (including the Sub-Processors) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(m) Client hereby grants Templum general written authorization to engage the Sub-Processors set forth in Appendix 1. Templum shall inform Client of any changes concerning the addition or replacement of Sub-Processors in writing at least thirty (30) business days in advance. If Client notifies Templum in writing of any objections to such changes, the Parties shall work in good faith to find a commercially reasonable, mutually agreeable resolution to such objection. Templum shall require the Sub-Processors who are provided access to, or otherwise come into contact with, Client Personal Information to protect all such Client Personal Information including by entering into a written contract, which includes terms at least substantively the same as the terms of this Addendum.

(n) Templum agrees and warrants that it will implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing of the Personal Data, which are designed to comply with Applicable Privacy Laws and protect against the unauthorized or unlawful processing, accidental loss, destruction, or damage of information such as Client Personal Information and ensure the protection of the rights of Data Subjects under Applicable Privacy Laws.

(o) To the extent the SCCs or UK Addendum apply, the Parties hereby acknowledge and agree that Templum shall make available to Client all information necessary to demonstrate Templum's compliance with the obligations laid down in this Addendum and allow for and contribute to audits, pursuant to Clause 8.9 of the SCCs.

(p) On Client's written request at termination or expiration of the Agreement, Templum shall promptly and securely destroy and confirm such destruction of all Client Personal Information in its possession or control. Notwithstanding the foregoing, the Templum shall retain the Client Personal Information only for as long as necessary to perform the Services, or as otherwise required or permitted by any Applicable Privacy Laws or other applicable laws, regulation, or professional standards. Any Client Personal Information so kept shall be maintained in accordance this Addendum and only processed to the extent and for as long as required for such purposes.

APPENDIX 1 TO DATA PROTECTION ADDENDUM

1. LIST OF PARTIES

a. Client (as defined in this Addendum) shall, to the extent the SCCs apply, act as data exporter

   i. Client address, contact person: As set forth in the main body of the Agreement

   ii. Activities: Use of technology services pursuant to the Agreement

   iii. Role (controller/processor): Controller

b. Templum shall, to the extent the SCCs apply, act as data importer

   i. Templum address, contact person: As set forth in the main body of the Agreement

   ii. Activities: Performance of technology services pursuant to the Agreement

   iii. Role (controller/processor): Processor

2. DESCRIPTION OF TRANSFER

a. Categories of Data Subjects whose Client Personal Information is provided to Templum in connection with its performance of the Services:

   - Individuals who do business with Templum's clients

b. Categories of Client Personal Information (e.g., Social Security Numbers, dates of birth, or home addresses) provided to Templum in connection with its performance of the Services:

   - Personal identifiable information (such as name, home or work address, email address, location data and government issued identification).
   - Personal financial information (such as financial accounts of persons, bank accounts, investment accounts and payroll records).

c. Sensitive data transferred (if applicable): None, except to the extent expressly agreed by the parties in this Appendix or the applicable Statement of Work agreed by the Parties in accordance with the main body of the Agreement (if any). For this purpose, "**sensitive data**" means Client Personal Information 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 or offences.

d. Frequency of the transfer (e.g., whether the Client Personal Information is transferred on a one-off or continuous basis):

   - As needed to facilitate performance of the Services in accordance with the Agreement.

e. Nature and purpose(s) of the processing:

   i. When Templum processes Client Personal Information as a Processor, Templum shall do so in accordance with Templum's obligations under Article 28 of the GDPR as set forth in this Addendum and the SCCs (to the extent applicable), and solely for the purposes permitted under this Addendum and/or the Agreement, including to perform the Services and as required by applicable law, regulation, or professional standards.

f. Period for which the Client Personal Information will be retained:

   - Until such Client Personal Information is returned or destroyed in accordance with and subject to the terms of this Addendum.

g. Templum may transfer Client Personal Information to the following third countries or international organizations outside the EEA or UK:

   - The United States of America

h. Templum is authorized to engage the following Sub-Processors in accordance with the terms of this Addendum and the Agreement:

   i. Microsoft Azure (i.e. https://azure.microsoft.com/en-us)

   ii. Onfido (i.e. https://onfido.com/)

   iii. Datadog (i.e. http://datadoghq.com)

3. COMPETENT SUPERVISORY AUTHORITY

i. To the extent the SCCs apply, the competent supervisory authority shall be determined in accordance with SCC Clause 13(a).

APPENDIX 2 TO DATA PROTECTION ADDENDUM

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. **Program**. Service Provider will implement and maintain a comprehensive written information security program ("Information Security Program"), which contains appropriate administrative, technical and organizational safeguards designed to protect the security, integrity, availability, resilience and confidentiality of Client's Confidential Information and that meet or exceed generally accepted industry standards.

2. **Access Controls**. Service Provider will: (a) abide by the "principle of least privilege," pursuant to which Service Provider will permit access to Client's Confidential Information by its personnel on a need-to-know basis; and (b) be responsible for any processing of Client's Confidential Information by its personnel within the scope of the provided Services.

3. **Account Management**. Service Provider will use reasonable measures to manage the creation, use, and protection of all account credentials used to access the Service Provider Systems, including by implementing: (a) a segregated account with unique credentials for each user; (b) strict management of administrative accounts; (c) password best practices, including the use of strong passwords and secure password storage; and (d) periodic review of entitlements and credentials. "Service Provider Systems" means the facilities, systems, equipment, hardware, and software used in connection with Service Provider's processing of Client's Confidential Information.

4. **Vulnerability Management**. Service Provider will: (a) use automated vulnerability scanning tools to periodically scan the Service Provider Systems; (b) log vulnerability scan reports; (c) use patch management and software update tools for the Service Provider Systems as appropriate; (d) prioritize and remediate vulnerabilities according to severity, as assessed by Service Provider; and (e) use compensating controls if no patch or remediation is immediately available. The patching of Service Provider Systems will be completed within a timeframe in alignment with the known abilities to exploit the vulnerability, and the overall risk level, unless Service Provider determines that appropriate mitigation controls are in place or when there would be a significant impact to business operations.

5. **Incident Response**. Service Provider will notify Client of any occurrence that results in material harm to the confidentiality, integrity, or availability of Client Confidential Information ("Security Incident") within seventy-two (72) hours of such Security Incident, and in any event within the time required by applicable law, after confirming that a Security Incident has occurred. In any such notice, Service Provider will include a summary of: (a) the Security Incident, (b) any ongoing risks to the Client Confidential Information that the Security Incident poses, and (c) the measures taken by Service Provider to address the Security Incident. The contents of the summary may be provided in phases, and in no event will Service Provider be required to provide information that in Service Provider's sole judgement would present a security or legal risk to Service Provider. Service Provider will provide reasonable

assistance to Client to investigate, remediate or take any other action that Client deems reasonably necessary regarding the Client's internal remediation of the Security Incident, including in connection with any dispute, inquiry, investigation or claim concerning the Security Incident, to the extent the Security Incident is not at least partially attributable to the actions or omissions of Client, Client's employees, Client's agents, or Client's plan participants.

6. **Security Segmentation**. Service Provider will use reasonable measures to monitor, detect and restrict the flow of information on a multi-layered basis within the Service Provider Systems using tools such as firewalls, proxies, and network-based intrusion detection systems will continuously maintain industry-standard firewall protection for the System. Service Provider will test its perimeter router and firewall devices on a regular basis, and not less than commercially reasonable to identify unsafe configurations and vulnerabilities.

7. **Data Loss Prevention**. Service Provider will use reasonable data loss prevention measures to identify, monitor and protect Client's Confidential Information. Such data loss prevention processes and tools will include: (a) automated tools to identify attempts of data exfiltration; (b) the secure and managed use of portable devices; (c) use of certificate-based security; and (d) secure key management policies and procedures.

8. **Encryption**. Service Provider will encrypt, using industry standard encryption tools, Client's Confidential Information that Service Provider transmits or sends wirelessly or across public networks. Service Provider will safeguard the security and confidentiality of all encryption keys associated with encrypted information.

9. **Secure Software Development**. Service Provider implements controls designed to ensure that any software used in connection with the processing of Client's Confidential Information is or has been developed using secure software development practices as appropriate, which can include: (a) segregating development and production environments; (b) filtering out potentially malicious character sequences in user inputs; (c) using secure communication techniques, including encryption; (d) using sound memory management practices; (e) using web application firewalls to address common web application attacks such as cross-site scripting, SQL injection and command injection; (f) implementing the OWASP Top Ten recommendations, as applicable; (g) patching of software; and (h) testing object code and source code for common coding errors and vulnerabilities using code analysis tools.

11. **Administrative Safeguards**. Prior to providing access to Client's Confidential Information to any of its personnel, Service Provider will: (a) ensure the reliability of such personnel, including by performing background screening (to the extent permitted by Data Protection Law); and (b) provide appropriate security training to such personnel to ensure such personnel can comply with the obligations under this Addendum. Service Provider will periodically provide additional training to its personnel as may be appropriate to help ensure that Service Provider's Information Security Program meets or exceeds prevailing industry standards.

12. **Subcontractors**. To the extent that Service Provider uses subcontractors or other third parties pursuant to fulfilling its obligations under the Agreement, and those subcontractors or third parties receive access to Client's Confidential Information, Service Provider shall require the subcontractors or third parties to adhere to security obligations appropriate for the subcontractor's scope of work. Service Provider shall perform due diligence on its subcontractors and third parties to confirm compliance with information security obligations.

13. **Penetration Testing**. Service Provider shall conduct a penetration test on its public facing systems no less than once annually and will provide confirmation of the same if requested by Client.

14. **Business Continuity Management**. Service Provider has documented procedures for business continuity, IT service continuity, and incident management, designed to restore the Services as quickly as practical, in the event of an incident that prevents Service Provider from providing the Services. Service Provider may unilaterally revise and update its documented procedures at any time.

15. **Limited Audit**. No more than once annually upon written request by Client, Service Provider shall make available to Client a written statement that it has complied with all of the requirements of this Addendum, as well as a written overview of Service Provider's information security controls. Client may, no more than once annually, submit a reasonable request for information to Service Provider related to Service Provider's Information Security Program. Service Provider will provide responses to the requests, but in no circumstance will Service Provider be required to provide any information that, in Service Provider's sole judgment, could present a security risk to the Information Security Program, to Service Provider, or to Service Provider's clients.

16. **Cybersecurity Insurance**. Service Provider intends to maintain, and will continue to maintain once purchased, for the duration of the Agreement, a cyber insurance policy that covers losses related to cybersecurity incidents. No more than once annually, Service Provider shall provide the Client with a certificate of insurance upon Client's request.