<u>EU GENERAL DATA PROTECTION REGULATION ADDENDUM</u>

This European Union General Data Protection Regulation Addendum to the [AGREEMENT NAME] (this "**Addendum**") is made and entered into as of the ___ day of _____, 20__ (the "**Addendum Effective Date**") by and between the parties identified below:

KENT STATE UNIVERSITY
800 E. Summit St.
Kent, OH 44242

VENDOR
[FULL LEGAL NAME]
[ADDRESS OF
PRINCIPAL OFFICES]

Date of [Agreement Name] ("Vendor Agreement"): [Date of Agreement]

WHEREAS, **Kent State University** ("KENT STATE") and [**VENDOR NAME]** ("Vendor") entered into that certain Vendor Agreement referenced above for Vendor to provide professional services, software services, and/or other services (collectively, the "**Services**");

WHEREAS, Vendor may acquire, access, or otherwise Process Personal Data in performing and/or providing the Services;

WHEREAS, KENT STATE and Vendor desire to protect the Personal Data in accordance with all applicable data protection laws and industry best practices, including, but not limited to, the General Data Protection Regulation (EU) 2016/679 and any successor legislation imposing equivalent obligations.

NOW, **THEREFORE**, in consideration of the mutual agreements and covenants contained herein, together with other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, KENT STATE and Vendor agree as follows:

1. **<u>Defined Terms</u>**. Capitalized terms used in this Addendum that are not otherwise defined herein will have the same meaning ascribed to them as set forth in the Vendor Agreement. As used herein, the term "Agreement" refers to the terms and conditions of both the Vendor Agreement and this Addendum in effect following the Addendum Effective Date.

   a. "**Appropriate Safeguards**" means technical, physical, and organizational measures, standards, requirements, specifications, or obligations designed to ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected, taking into account the state of the art; costs of implementation; the nature, scope, context, and purposes of Processing; and the risk of varying likelihood and severity for the rights and freedoms of natural persons. Appropriate Safeguards shall, at minimum, be at levels commensurate with at least one information security standard framework selected by Vendor from the following: (i) Privacy & IT Security Best Practices (as defined by the International Organization for Standardization's ISO 27001); (ii) the Information Systems Audit and Control Association's Control Objectives for Information and Related Technology 5; or (iii) the U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800 series.

   b. **"Data Protection Laws"** means all data protection laws applicable to the Processing of Personal Data under this Agreement, including local, state, national and/or foreign laws, treaties, and/or regulations, laws of the European Union and European Economic Area, and implementations of the GDPR into national law.

c. **“GDPR”** refers to the General Data Protection Regulation (EU) 2016/679 and any successor legislation imposing equivalent obligations.

d. “**Personal Data**” means any information relating to an identified or identifiable natural person (“data subject”), to the extent that such personal data are associated with European Economic Area residents or are otherwise within the scope of the GDPR. An identifiable 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, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. “Personal Data” includes, but is not limited to, addresses, phone numbers, passport numbers, driver’s license numbers, user names, passwords, credit or debit card numbers, bank account numbers, other financial account numbers, personal identification numbers, dates of birth, Social Security numbers, IP addresses, biometric information, health data, and other unique identification information. For the avoidance of doubt, the meaning of “Personal Data” shall be consistent with the term as it is defined in Article 4(1) of the GDPR.

e. “**Processing, Process, Processed**” means 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. For the avoidance of doubt, the meaning of “Processing, Process, Processed” shall be consistent with the term as it is defined in Article 4(2) of the GDPR.

f. “**Remediation Efforts**” means, with respect to any Security Incident, activities designed to remedy a Security Incident which may be required by applicable law or by KENT STATE’s policy or procedures, or which may otherwise be necessary, reasonable or appropriate under the circumstances, commensurate with the nature of such Security Incident. Remediation Efforts may include: (i) development and delivery of legal notices to affected individuals or other third parties as may be required by applicable law or as otherwise appropriate; (ii) establishment and operation of toll-free telephone numbers (or, where toll-free telephone numbers are not available, dedicated telephone numbers) for affected individuals to receive specific information and assistance; (iii) provision of free credit reports, credit monitoring and credit or identity repair services for affected individuals; (iv) provision of identity theft insurance for affected individuals; (v) cooperation with and response to regulatory inquiries and other similar actions; (vi) undertaking of investigations of such Security Incident; and (vii) cooperation with and response to litigation with respect to such Security Incident.

g. “**Security Incident**” means (i) any incident leading to the actual or suspected unauthorized, accidental, or unlawful use of, loss of, alteration to, disclosure of, or access to, any Personal Data transmitted, stored, or otherwise Processed; and (ii) any security breach, incident, or event (or substantially similar term) as defined by applicable Data Protection Laws. A Security Incident may constitute a Personal Data Breach, as defined in GDPR Article 4(12).

h. “**Subprocessor**” means any third party that Vendor engages in accordance with Section 2(c) of this Addendum in order to perform the Processing.

i. "**Valid Transfer Mechanism**" means any data transfer mechanism recognized by the European Commission as a legitimate basis for the transfer of Personal Data outside the European Economic Area.

2. **Vendor Obligations**.

a. Data Use. In accordance with GDPR Article 28(3), Vendor shall Process the Personal Data only: (i) for the purpose of performing the Services during the term of this Agreement; (ii) pursuant to documented instructions from KENT STATE, including with respect to transfers of Personal Data to a third country or international organization; or (iii) when required to do so by applicable law, and the Vendor informs KENT STATE of that legal requirement before Processing, unless that law prohibits the disclosure to KENT STATE on important grounds of public interest. Vendor shall disclose Personal Data only to Vendor employees that have a need to know the same for the performance of the Processing and have either expressly committed to protecting the confidentiality of such data or are under an appropriate statutory obligation of confidentiality.

b. Appropriate Safeguards. Vendor represents and warrants that in accordance with GDPR Article 28(1), it has implemented Appropriate Safeguards in such a manner that its Processing will meet the requirements of the GDPR; ensure the ongoing confidentiality, integrity, and availability, and resilience of Processing systems and activities; and ensure the protection of the rights of the data subjects. In determining which Appropriate Safeguards to apply, Vendor has considered the risks that are presented by the Processing activities, such as the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to the Personal Data. Appropriate Safeguards include, but are not be limited to, the following:

i. *Encryption, Anonymization, and Pseudonymization*. When reasonable and appropriate, Vendor shall encrypt Personal Data that is either in storage or transmission, anonymize Personal Data, or pseudonymize Personal Data.

ii. *Asset Management*. Vendor shall create and maintain an inventory of all information technology (IT) assets utilized by Vendor to Process Personal Data. Such inventory shall designate an owner for each IT asset.

iii. *Human Resources Security.* Vendor shall inform all personnel of Vendor's security obligations under the Agreement and conduct identity verification and a reasonable pre-employment due diligence screening of such personnel prior to such personnel performing any aspect of the Services. Any Vendor personnel accessing KENT STATE's facilities shall conform to KENT STATE's security policies and procedures and agree to undertake KENT STATE security training as may be requested from time to time.

iv. *Physical and Environmental Security*. Vendor shall use reasonable and appropriate security measures to protect its facilities and any equipment and devices therein that store or transmit Personal Data from unauthorized physical access, tampering, or theft.

v. *Communications and Operations Management*. Vendor shall deploy anti-virus software on all systems commonly affected by computer viruses and/or malicious code. Vendor shall use commercially reasonable efforts to maintain such anti-virus software, including the identification and installation of anti-virus signature updates on a daily basis and periodic execution of automatic scans. Vendor shall implement and maintain firewalls at the network perimeter between Vendor's internal (private) and public (Internet) networks. Vendor shall deploy intrusion detection systems and/or intrusion prevention systems such that all egress points are actively monitored. The information systems used for the purposes of Processing Personal Data must have only those services/processes and ports enabled that are essential to perform routine business. Vendor shall utilize encrypted communication channels at all times for inter-host communications to external or untrusted networks.

vi. *Access Controls*. Vendor shall implement the following access controls on any computer system associated with the Service: (1) user authentication must use unique identifiers ("User ID") for each individual; (2) robust password policy must be enforced for each User ID; (3) user access rights/privileges to information resources containing Personal Data must be granted on a need-to-know basis consistent with role-based authorization; (4) user access to Personal Data must be removed immediately upon user separation or role transfer eliminating valid business need for continued access; and (5) default passwords and security parameters must be changed in third-party products/applications used to support Personal Data.

vii. *Business Continuity Management*. Vendor will maintain a business continuity plan that will enable it to restore, in a timely manner, the availability of and access to Personal Data in the event of a physical or technical incident resulting in a service interruption. Vendor shall restore the Services to a condition where such Services conform to the requirements set forth in the Agreement. If an incident or service interruption occurs, Vendor shall promptly notify KENT STATE of the nature and scope of the event and implement its business continuity plan. Within a reasonable time thereafter, Vendor shall inform Company of the steps that Vendor has taken in an effort to remediate the impact of the service interruption, including, if applicable, attempts to restore any lost Personal Data.

c. Subprocessors. KENT STATE acknowledges and agrees that Vendor may engage Subprocessors to Process Personal Data. Subcontractors are permitted to Process Personal Data only to deliver the Services, and are prohibited from Processing Personal Data for any other purpose. Vendor shall not engage a Subprocessor without obtaining prior specific or general written authorization from KENT STATE in accordance with GDPR Article 28(2). If KENT STATE grants Vendor a general written authorization to engage Subprocessors, then Vendor shall inform KENT STATE of any intended changes regarding the addition or replacement of other Subprocessors such that KENT STATE will receive an opportunity to object to such changes. Additionally, in accordance with GDPR Article 28(4), Vendor shall enter into a written contract or other legally binding agreement with Subprocessor imposing the same data protection obligations set forth in this Addendum upon the Subprocessor and requiring the Subprocessor to provide sufficient guarantees to implement appropriate technical and organizational measures in a manner that allows the Processing to meet the requirements of the GDPR and ensure the protection of the rights of the data subjects. Vendor shall be liable for the Subcontractor's acts and omissions to the same extent as if such acts and omissions were performed by Vendor.

d. Security Incidents. Vendor shall notify KENT STATE by email and by phone of any potential or actual Security Incident within seventy-two (72) hours of Vendor becoming aware of such Security Incident. Vendor shall investigate any such Security Incident and take all necessary steps to eliminate or contain the exposures that led to such Security Incident in accordance with the Appropriate Safeguards and applicable laws. Vendor shall provide KENT STATE with a written report within five days of the occurrence of any Security Incident, describing the nature and categories of the Personal Data involved in the incident; the approximate number and categories of data subjects affected by the incident; contact information for an individual at the Vendor from whom more information can be obtained; the likely consequences of the incident; and steps taken by Vendor to mitigate the harmful effects of the incident. If it is not possible for Vendor to provide the complete report to KENT STATE at the same time, then Vendor may provide such information in phases without undue further delay. Additionally, Vendor shall: (i) at KENT STATE's sole discretion, either undertake Remediation Efforts at its sole expense or reimburse KENT STATE for reasonable costs and expenses in connection with taking Remediation Efforts; and (ii) ensure that the plan associated with such Remediation Efforts includes components aimed at preventing the recurrence of the same type of Security Incident.

e. **Data Subjects' Rights.** To the extent reasonably practicable, Vendor shall implement the necessary technical and organizational measures to facilitate KENT STATE's fulfillment of its obligations related to the exercise of the data subjects' rights as described in GDPR Articles 12–20. Vendor agrees to promptly notify KENT STATE of any requests it receives directly from data subjects concerning the exercise of their rights as described in GDPR Articles 12–20.

f. **Record Retention**. Vendor shall maintain all records related to its Processing activities performed on behalf of KENT STATE that are required by GDPR 30(2).

g. **Evaluations**. In accordance with GDPR Article 32(1)(d), Vendor shall regularly evaluate, test, and assess the effectiveness of the Appropriate Safeguards for ensuring the security of the Processing. Vendor shall promptly adjust and/or update the Appropriate Safeguards as reasonably warranted by the results of such evaluation, testing, and monitoring (collectively, an "Evaluation"). Each Evaluation shall include, at a minimum, an assessment of its implementation and maintenance of Appropriate Safeguards and compliance with applicable law for the purpose of issuing a SSAE 16 SOC 2 Type II report, AT 101 report, or other comparable independent attestation from a nationally-recognized, independent ("Evaluation Report"). Upon KENT STATE's reasonable request, Vendor shall provide a copy of its most recent Evaluation Report. If the Evaluation Report is qualified, Vendor shall submit, in addition to the report, a plan describing actions that Vendor will implement to correct the situation that caused the auditor to issue a qualified Audit Report, a timetable for implementing the planned corrective actions and a process for monitoring compliance with the timetable. Vendor shall promptly respond to and remediate the deficiencies identified, and implement any changes suggested by the auditor.

h. **Audit Rights.** Vendor shall permit KENT STATE, or a third party retained by KENT STATE, to perform reasonable audits of Vendor's operations, processes, policies, and documents: (i) to the extent they relate to the exceptions reported in the Evaluation Report described in Section 2(d); (ii) if there is a Security Incident; or (iii) to verify Vendor's compliance with the terms of this Agreement and the obligations set forth in GDPR Article 28 pertaining to the Processing of Personal Data. Such audits shall be conducted during Vendor's normal business hours, upon reasonable prior notice, and no more frequently than once per year during the term of this Agreement, unless in response to a Security Incident or otherwise agreed to by the parties. Additionally, upon KENT STATE's reasonable request, Vendor shall make available all information necessary to demonstrate compliance with the obligations set forth in GDPR Article 28.

i. **Data Return or Destruction**. At KENT STATE's discretion, Vendor shall destroy or return all Personal Data to KENT STATE immediately upon the expiration or termination of this Agreement. Vendor shall also delete all existing copies of Personal Data in its possession, unless applicable EEA member state law requires their continued storage. If Vendor destroys Personal Data, it shall ensure that any residual magnetic, optical, or electrical representation of Personal Data that has been deleted may not be retrieved or reconstructed when storage media is transferred, becomes obsolete, or is no longer usable or required under the Agreement. Further, Vendor shall: (1) render data unreadable when storage is reused, recycled, disposed of, or accessed by any means outside of authorized applications; (2) ensure that data retention and destruction aligns with KENT STATE's requirements and policies as well as comply with applicable laws or regulations; and (3) ensure Personal Data stored on Vendor media (e.g., hard drive, optical discs, tapes, paper, etc.) is rendered unreadable or unattainable in accordance with the NIST Guidelines for Media Sanitization (Special Pub 800-88) prior to the media being reused, recycled or otherwise disposed. If any third party services are used for data destruction, Vendor shall provide to KENT STATE a certificate of destruction.

j. Facilitating KENT STATE's GDPR Compliance. To the extent reasonably practicable, Vendor shall assist KENT STATE in complying with its obligations related to Security Incidents, as described in GDPR Articles 33–34; data protection impact assessments, as described in GDPR Article 35; and required prior consultations with the supervisory authority regarding potential Processing, as described in GDPR Article 36. Vendor shall also immediately inform KENT STATE if, in its opinion, an instruction from KENT STATE related to Processing would infringe the GDPR or other Data Protection Laws**.**

k. International Data Transfers. Vendor shall ensure that Personal Data is not transferred to, allowed access by, or otherwise Processed across national borders (whether performed by itself or by a Subcontractor), unless it receives documented instructions to make such transfer from KENT STATE and such transfer will comply with all applicable Data Protection Laws and Valid Transfer Mechanisms.

3. **Indemnification**. Vendor shall defend, indemnify, and hold harmless KENT STATE, its affiliates, and each of their officers, directors, employees, customers, contractors, and agents from and against any and all third party claims, expenses, costs (including reasonable attorneys' fees), penalties, settlements, and damages arising out of or related to Vendor's breach of its obligations set forth in this Addendum.

4. **Precedence**. This Addendum incorporates by reference all of the other terms and conditions of the Vendor Agreement which shall remain in effect. However, as agreed to herein, this Addendum modifies such terms and conditions to account for the protection of Personal Data. Accordingly, the parties hereby agree that to the extent the terms of this Addendum and the Vendor Agreement conflict with one another, the terms and conditions of this Addendum shall control.

IN WITNESS WHEREOF, the parties have caused this Addendum to be signed by their respective duly authorized representative as of the date listed below.

Kent State University

Signed: ______________________________

Name: ______________________________

Title: ______________________________

Date: ______________________________

[VENDOR NAME]

Signed: ______________________________

Name: ______________________________

Title: ______________________________

Date: ______________________________