**GDPR DATA PROTECTION ADDENDUM**

This GDPR Data Protection Addendum (“**Addendum**”) is made and entered into effective as of **[ ] (**the “**Effective Date**”) by and between **The University of Texas System**, a state agency and institution of higher education established under the laws of the State of Texas (“**University**”) and **[ ]** (“**Contractor**”), (collectively, “**Parties**”). The purpose of this Addendum is to provide the terms related to privacy, confidentiality, and security which Contractor is required to adhere to, under applicable Data Protection Laws and Regulations, in order to process, handle, and store Personal Information on behalf of University as set forth in the Standard Agreement (“**Underlying Agreement**”).

1. **Definitions**
2. “GDPR” means the European Union (EU) General Data Protection Regulation, EU 2016/679 of the European Parliament and of the Council.
3. “Personal Information” means any and all data obtained directly from an individual or included in University Records (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. Personal Information includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data, “personal data” (as defined in the GDPR) and any and all information about an individual’s computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person’s online activities, browsing, application or hotspot usage or device location.
4. “Privacy Laws” means all applicable U.S. and international laws that regulate the Processing of Personal Information. In particular, “Privacy Laws” includes the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the Identify Theft Enforcement and Protection Act (ITEPA), the GDPR and other applicable laws that specify privacy, security or security breach notification obligations that affect the Personal Information or the provision of the services by Contractor.
5. “Process” or “Processing” means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, transfer, transmission, combination, redaction, erasure, or destruction.
6. “Security Breach” means a “personal data breach” (as defined in the GDPR), a “breach of the security of a system” or similar term (as defined in any other applicable Privacy Law) or any other event that compromises the security, confidentiality or integrity of Personal Information.
7. “Sensitive Personal Information” is a subset of Personal Information, which due to its nature has been classified by law or by University policy as deserving additional privacy and security protections. Sensitive Personal Information consists of: (i) all government-issued identification numbers, (ii) all financial account numbers (including payment card information and health insurance numbers), (iii) individual medical records, genetic and biometric information, (iv) all data obtained from a U.S. consumer reporting agency (such as employee background investigation reports, credit reports, and credit scores), (v) user account credentials, such as usernames, passwords, security questions/answers and other password recovery data, (v) data elements that constitute “Special Categories of Data”, as defined by Article 9 under the GDPR, namely “Personal Information” revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
8. “Services” means any and all services that University requests the Contractor to perform under the Underlying Agreement.
9. “Subprocessor” means any third party (including Contractor’s affiliates, agents, and subcontractors) that provides any services to Contractor and that may have access (including inadvertent access) to any Personal Information.
10. “Transfer” means to disclose or otherwise make the Personal Information available to a third party (including to any affiliate or Subprocessor of Contractor), either by physical movement of Personal Data to such third party or by enabling access to Personal Data by other means.
11. **Contractor Obligations**
12. Contractor will only Process or Transfer Personal Information as authorized by University and as necessary to perform the Services detailed in the Underlying Agreement.
13. Contractor will promptly inform University in writing:

(i) if it is not in compliance with or cannot comply with any material term of this Addendum or of the Underlying Agreement, including any such term regarding the Services. In addition to any other rights of the University under this Addendum, the Underlying Agreement, or applicable law or regulation, in the event of such notice University at its sole discretion may (1) permit Contractor to use reasonable efforts to remedy any such non-compliance or (2) terminate Contractor’s further Processing of Personal Information under this Addendum and the Underlying Agreement;

(ii) of any request for access to any Personal Information received from an individual who is (or claims to be) the subject of the data;

(iii) of any request for access to any Personal Information received by Contractor from any government agency, entity, or official (including any data protection agency or law enforcement agency);

(iv) of any other requests with respect to Personal Information received from University or other third parties, other than those set forth in the Underlying Agreement. Contractor understands that it is not authorized to and will not respond to the requests identified in items (ii), (iii), and (iv) above, unless Contractor is (1) explicitly authorized by University or (2) the response is legally required under a subpoena or similar legal document issued by a government agency, entity, or official that compels disclosure by Contractor.

1. If Services involve Contractor’s collection of Personal Information directly from individuals, Contractor will provide the individuals with a clear and conspicuous written privacy notice, which notice will be reviewed by University before Contractor begins providing any Services set forth in the Underlying Agreement. The notice must comply with any legal requirements for the privacy notice in the jurisdictions where it is given, be translated into the languages used in connection with Contractor’s interaction with the individuals, and indicate that Contractor is processing Personal Information as a processor on behalf of University.
2. If the Personal Information includes “protected health information” (or “PHI”) as defined in the Health Insurance Portability and Accountability Act and 45 Code of Federal Regulations (CFR) Part 160 and subparts A and E of Part 164 (collectively, HIPAA)”), then before Contractor may receive, maintain or create any Personal Information, Contractor will execute an appropriate Business Associate Agreement (“BAA”) as required by HIPAA with University. To the extent that the BAA conflicts with any term contained in this Addendum or the Underlying Agreement, the terms of the BAA will control.
3. Subject to Section 2(b) of this Addendum, Contractor will cooperate with University and with its affiliates and representatives in responding to inquiries, incidents, claims and complaints regarding Processing of Personal Information or as otherwise needed for University to (1) demonstrate compliance with applicable Privacy Laws and (2) respect individuals’ rights under those Privacy Laws.
4. Contractor must use reasonable efforts to stay informed of applicable legal and regulatory requirements for Processing of Personal Information. Contractor will ensure that its Processing complies with all applicable Privacy Laws, as well as Contractor’s and University’s privacy notices.

**3.** **Confidentiality and Data Access**

1. Personal Information is considered Confidential Information of University.  Contractor will not use or disclose Personal Information received from or on behalf of University, its students, faculty, or staff, or any third party pursuant to the Underlying Agreement, (including any Personal Information provided by a University student directly to Contractor), except as permitted or required by the Underlying Agreement or this Addendum. If Contractor discloses any Personal Information to a Subprocessor Contractor will require the Subprocessor to comply with the same restrictions and obligations that are imposed on Contractor by the Underlying Agreement and this Addendum, including requiring each Subprocessor to agree to the same restrictions and obligations in writing.
2. Contractor will use the administrative, technical and physical security measures, including secure encryption in the case of electronically maintained or transmitted Personal Information, approved by University and that are at least as stringent as the requirements of UT System Information and Resource Use & Security Policy, UTS 165 at <http://www.utsystem.edu/board-of-regents/policy-library/policies/uts165-information-resources-use-and-security-policy>, to preserve the confidentiality and security of all Personal Information received from or on behalf of University, its students, faculty, or staff, or any third party pursuant to the Underlying Agreement.
3. Contractor has implemented and will maintain documented appropriate business continuity and disaster recovery plans to enable it to continue or resume providing Services in accordance with the Underlying Agreement in the event of any disaster or other adverse event affecting the University and/or Contractor.
4. Prior to allowing any employee, subcontractor, representative, agent, subprocessor, or other individual to process Personal Information, Contractor will (i) conduct an appropriate background check of the individual as permitted by law and in compliance with the Underlying Agreement, (ii) require the individual to execute an enforceable confidentiality agreement, and (iii) provide the individual with appropriate privacy and security training. Contractor will also continually monitor its employees, subcontractors, representatives, agents, subprocessors, or other individuals it provides or engages for compliance with the privacy and security program requirements.
5. Contractor, within 24 hours after discovery, will report to University any use or disclosure of Personal Information not authorized by this Addendum or the Underlying Agreement. Contractor’s report will identify: (i) the nature of the unauthorized use or disclosure, (ii) the Personal Information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Contractor has done or will do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or will take to prevent future similar unauthorized use or disclosure. Contractor will provide such other information, including written reports, as reasonably requested by University.
6. Upon request, Contractor will provide University with information about the Contractor’s information security program. Contractor will also submit its data processing facilities for audit, during Contractor’s reasonable business hours, which will be carried out in a mutually-agreeable manner no more than ten (10) days after such request. In the event that such audit reveals material gaps or weaknesses in Contractor’s security program, University will be entitled to terminate Contractor’s Processing of Personal Information, including, termination of this Addendum and the Underlying Agreement permanently, or until such issues are resolved.
7. **Return of Records**

Contractor agrees that no later than 30 days after expiration or termination of the Underlying Agreement or this Addendum for any reason, or within thirty (30) days after University’s written request, Contractor will halt all access, use, or processing of Personal Information and will return to University all records, including any copies created by Contractor or any Subprocessor, subcontractor, representative, agent, or other individual or entity that it provides or engages; and Contractor will certify in writing to University that all records have been returned to University.

**5. General Provisions**

This Agreement is governed by, and shall be construed in accordance with, applicable federal law and the laws of the State of Texas without regard to choice of law principles.

Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party’s address given below, and/or (other than for the delivery of fees) via facsimile to the facsimile telephone numbers listed below.

If to University:

The applicable U.T. Institution(s)’s Privacy/Data Protection Officer.

With copy to:

The University of Texas System Privacy and Data Protection Officer

Office of Systemwide Compliance

210 West 7th Street

Austin, Texas 78701

If to Contractor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Each Party named above may change its address and that of its representative for notice by the giving of notice thereof in the manner herein above provided.

**AGREED TO AND SIGNED BY THE PARTIES.**

**The University of [Contractor]**

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_