

Data Protection Addendum

This Data Protection Addendum supplements the University of Missouri Standard Procurement Terms and Conditions found at [PO Terms & Conditions](#) ("Terms and Conditions"). The Curators of the University of Missouri ("University") requires that their service providers, suppliers, distributors and other business partners and their employees (collectively "Contractor") comply with the requirements in this Data Protection Agreement ("DPA") with respect to any information that University, University employees, representatives, customers, or other business partners make available to Contractor in the context of Contractor's business relationship with University (collectively "University Data"). Contractor is a Processor that provides certain services ("Services") to University pursuant to an agreement or agreements with University (the "Underlying Agreement(s)") and Processes, on University's behalf, Personal Information that is necessary to perform the Services under the Underlying Agreement(s); and

1. Definitions

Any capitalized term used but not defined herein shall have the meaning ascribed to it in the applicable Data Protection Laws.

The definitions enumerated below (including all conjugations, forms, and tenses thereof) apply to this DPA:

- a. "Data Breach " means Contractor's negligence or a breach of Contractor's security measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information.
- b. "Data Protection Laws" means, as applicable: (a) the Family Educational Rights and Privacy Act (FERPA); (b) the Health Insurance Portability and Accountability Act (HIPAA); (c) the Gramm-Leach-Bliley Act (GLBA); (d) the Payment Card Industry Data Security Standards (PCI-DSS); (e) the Federal Export Administration Regulations, Federal Acquisitions Regulations, Defense Federal Acquisitions Regulations and Department of Education guidance; and (f) any other laws, rules, regulations, self-regulatory guidelines, implementing legislation, or third party terms relating to privacy, security, breach notification, data protection, or confidentiality and applicable to processing of Personal Information.
- c. "Data Subject" means any person, household, or device that becomes subject in any manner to the services performed for University by Contractor.
- d. "Personal Information" (i) means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Data Subject that may be (a) disclosed or otherwise made accessible to Contractor by University in anticipation of, in connection with, or incidental to the performance of Services for or on behalf of University; (b) Processed at any time by

Contractor in connection with or incidental to the performance of this DPA or the Underlying Agreement(s); or (c) derived by Contractor from the information described in a) or b) above; and (ii) supplements the foregoing definition enumerated in (i) by also incorporating the definition of "Personal Information," "Personal Data," and "Non-Public Personal Information under Data Protection Laws. Personal Information includes without limitation behavioral characteristics and profiles. Personal Information includes Protected Health Information as defined under HIPAA.

- e. "Processing" means performing any operation (whether automated or manual, or through some combination) relative to Personal Information, including, without limitation, accessing, collecting, organizing, retaining, using, disclosing, storing, manipulating, adapting, analyzing, aggregating, categorizing, transmitting, destroying, and deriving or creating information from, Personal Information.

2. Processing Restrictions and Obligations

Contractor may Process Personal Information only as strictly necessary to deliver the Services pursuant to the Underlying Agreement(s). Without limiting the foregoing and to avoid any doubt, Contractor represents, warrants, and covenants as follows:

- a. Contractor is acting solely as a Processor with respect to Personal Information, and University has the exclusive authority to determine the purposes for and means of Processing the Personal Information.
- b. Contractor will Process Personal Information only (i) for a business purpose and (ii) on behalf of University, for the sole purpose of performing the Services specified in the Underlying Agreement(s), and Contractor will not collect, retain, use, disclose or otherwise Process Personal Information for any other purpose.
- c. Contractor will not sell Personal Information, or use or otherwise Process Personal Information for monetary or other valuable consideration.
- d. Contractor will not retain, use, disclose or otherwise Process Personal Information outside of the direct business relationship between Contractor and University.
- e. Contractor may not derive information from Personal Information for any purpose other than to perform Services under the Underlying Agreement(s).
- f. Contractor may not engage or communicate with a Data Subject in any way, whether directly or indirectly (including, without limitation, via interest-based advertising, mobile messaging, contextual online experiences, online ad-serving, email, telephone, social media, and location-aware technologies) except under written agreement between Contractor and University that specifies the means and methodology of, and limitations on, the media or communication channel in question

- g. Contractor will immediately inform University in writing of any requests with respect to Personal Information received from University's customers, consumers, employees or others. Contractor will cooperate with University as needed by University regarding Data Subject rights, including enabling (i) access to a Data Subject's Personal Information, (ii) delivering information about the categories of sources from which the Personal Information is collected, (iii) delivering information about the category of Processor that Contractor is, or (iii) providing information about the categories or specific pieces of a Data Subject's Personal Information that Contractor Processes on University's behalf, including by providing the requested information in a portable and, to the extent technically feasible, readily useable format that allows a Data Subject to transmit the information to another entity without hindrance.
- h. Upon University's request, Contractor will immediately delete a particular Data Subject's Personal Information from Contractor's records and direct any relevant contractors or agents to delete such Personal Information from their records. Contractor will delete such Personal Information in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization standards. If Contractor is unable to delete the Personal Information for reasons permitted under applicable Data Protection Laws, Contractor will (i) promptly inform University of the reason(s) for Contractor's refusal of the deletion request, (ii) ensure the privacy, confidentiality, and security of such Personal Information, and (iii) delete the Personal Information promptly after the reason for Contractor's refusal has expired.
- i. Contractor may only Process Personal Information for as long as the applicable Underlying Agreement(s), relationship, or arrangement between Contractor and University authorizes it, and only to benefit University (and not Contractor or any of Contractor's other clients or customers). In the event of any conflict with this DPA and any Business Associate Agreement ("BAA") between University and Contractor, the BAA will control.
- j. Where Contractor provides to a third party access to Personal Information, or contract any of Contractor's rights or obligations concerning Personal Information to a third party, Contractor will enter into a written agreement with each such third party that imposes obligations on the third party that are at least equivalent to those imposed on Contractor under this DPA. By written agreement and through technical, organizational, and physical measures, Contractor must (i) limit such third party's access to and Processing of Personal Information to that which is solely necessary to deliver the Services under the Underlying Agreement(s) and (ii) prohibit such third party from selling Personal Information.
- k. Contractor will maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, University Data), pursuant to applicable Data Protection Laws, and keep University Data confidential. Contractor will ensure that such

persons with access to University Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- l. Contractor will make its applicable employees familiar with the relevant provisions of the Data Protection Laws and shall provide adequate training. Contractor will supervise compliance of such employees with applicable Data Protection Laws.
- m. University has the right to audit Contractor's compliance with the Data Protection Laws, the Underlying Agreement(s) and this DPA (including the technical and organizational measures), by requesting information about and reasonably inspecting storage of the University Data, and implemented policies and security incident reports, subject to reasonable prior notice of at least ten (10) business days in advance and, to the extent reasonably possible, without interfering with Contractor's regular business operations. University and Contractor shall mutually agree upon the scope, timing and duration of the audit.
- n. In accordance with the Data Protection Laws and other industry standards, Contractor has appropriate policies and procedures in place to manage a Data Breach.
- o. In accordance with the Data Protection Laws, Contractor shall notify University without undue delay, but in no event later than 36 hours after discovery, in the event of a Data Breach relating to University Data, of which Contractor reasonably suspects or knows to have occurred. Contractor shall provide commercially reasonable cooperation and assistance in identifying the cause of the Data Breach and take all commercially reasonable steps to remediate the Data Breach to the extent within Contractor's control.
- p. Contractor will not process Personal Information outside of the United States without the prior written consent of University, which may be granted or denied by University in its sole discretion.
- q. Contractor will maintain a list of subcontractors and update such list prior to any engagement of any subcontractor and give University an opportunity to object to that subcontractor. If University objects to the subcontractor, Contractor will work with University in good faith to arrange for the performance of the Services without the use of such subcontractor and University may terminate this Agreement without penalty. Such engagement must be pursuant to a written contract that requires the subcontractor to also meet the obligations set forth in this Section for the Contractor
- r. With respect to any Data Breach due to Contractor or any subcontractor's action or inaction, notwithstanding anything to the contrary in the Underlying Agreement(s), and without regard to any limitations of liability contained in the Underlying Agreement(s), Processor shall indemnify University for the cost of a cyber forensic investigation, any required consumer regulator notices and related attorney fees and any other costs, fines, damages, and penalties incurred under Applicable Data Protection Laws.

- s. In addition to any other insurance coverage required by another contract/agreement with the University, the Contractor will for the duration of the term of the Underlying Agreement(s), maintain data breach coverage to cover claims arising out of the negligent acts, errors or omissions of Contractor, its subcontractors or anyone directly or indirectly employed by them. The coverage provided shall not be less than \$2,000,000 per occurrence, \$5,000,000 aggregate. Prior to the commencement of work under the Underlying Agreement(s), Contractor shall provide a certificate of insurance evidencing such insurance, shall name the officers, employees, and agents of The Curators of the University of Missouri as Additional Insured with respect to the order to which these insurance requirements pertain. Neither the requirement for Additional Insured status nor any of the Contractor's action in compliance with such requirement, either direct or indirect, is intended to be and neither shall be construed as a waiver of any sovereign immunity, governmental immunity or any other type of immunity enjoyed by University, the Board of Curators of the University of Missouri, or any of its officers, employees or agents. Contractor shall provide for notification to University within at least thirty (30) days prior to expiration or cancellation of such insurance. In the event the Contractor fails to maintain and keep in force the required insurance or to obtain coverage from its subcontractors, the University shall have the right to cancel and terminate the Underlying Agreement(s) upon written notice.

3. Compliance with Data Protection Laws

- a. Contractor and University acknowledge and agree that University does not sell Personal Information to Contractor in connection with any Agreement between Contractor and University. Contractor acknowledges and confirms that Contractor does not Process Personal Information from University in exchange for monetary or other valuable consideration, and that Contractor may not have, derive, or exercise any rights or benefits regarding Personal Information, except to Process the Personal Information as necessary to deliver Services to University pursuant to the Underlying Agreements.
- b. Upon the reasonable request of University, Contractor shall make available all information in its possession necessary to demonstrate compliance with any applicable Data Protection Law.
- c. Contractor will promptly notify University if Contractor determines that Contractor can no longer meet its obligations under this Section or any applicable Data Protection Law.
- d. The Parties acknowledge and agree that University has no knowledge or reason to believe that Contractor is unable to comply with the provisions of this DPA or any applicable provisions of the Data Protection Laws.
- e. Contractor certifies that Contractor understands and will comply with the requirements and restrictions set forth in this DPA, and with all applicable provisions of the Data Protection Laws.

- f. The following provision applies only if Contractor will have access to the University's education records as defined under FERPA: The Contractor acknowledges that for the purposes of this DPA it will be designated as a "school official" with "legitimate educational interests" in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Contractor agrees to abide by the limitations and requirements imposed on school officials. Contractor will use the education records only for the purpose of fulfilling its duties under the Underlying Agreement(s) and will not share such data with or disclose it to any third party except as provided for in this DPA, required by law, or authorized in writing by the University.
- g. If the Payment Card Industry Data Security Standard (PCI-DSS) is applicable to the Contractor service provided to the University, the Contractor agrees to:
 - i. Store, transmit, and process University Data in scope of the PCI DSS in compliance with the PCI DSS; and
 - ii. Attest that any third-party providing services in scope of PCI DSS under the Underlying Agreement(s) will store, transmit, and process University Data in scope of the PCI DSS in compliance with the PCI DSS; and
 - iii. Provide either proof of PCI DSS compliance or a certification (from a recognized third-party security auditing firm), within 10 business days of the request, verifying Firm/Vendor and any third party who stores, transmits, or processes University Data in scope of PCI DSS as part of the services provided under the Underlying Agreement(s) maintains ongoing compliance under PCI DSS as it changes over time; and
 - iv. Store, transmit, and process any University Data in scope of the PCI DSS in a manner that does not bring the University's network into PCI DSS scope; and
 - v. Attest that any third-party providing services in scope of PCI DSS under the Underlying Agreement(s) will store, transmit, and process University Data in scope of the PCI DSS in a manner that does not bring the University's network into PCI DSS scope.

4. Applicable Digital Accessibility Laws and Regulations

The University affords equal opportunity to individuals with disabilities in its employment, services, programs and activities in accordance with federal and state laws, including [28 C.F.R. Pt. 35](#). This includes effective communication and access to electronic and information communication technology resources, and the University expects that all products will, to the greatest extent possible, provide equivalent ease of use for individuals with disabilities as for non-disabled individuals. The University of Missouri has adopted the Web Content Accessibility

Guidelines (WCAG) 2.1 AA as the minimum standard, as specified by the implementing regulations of Title II of the Americans with Disabilities Act.

Contractor shall: (1) deliver all applicable services and products in reasonable compliance with University standards (Web Content Accessibility Guidelines 2.1, Level AA or above); (2) provide the University with an Accessibility Conformance Report detailing the product's current accessibility according to WCAG standards using the latest version of the Voluntary Product Accessibility Template (VPAT); (3) if accessibility issues exist, provide a "roadmap" plan for remedying those deficiencies on a reasonable timeline to be approved by the University; (4) promptly respond to assist the University with resolving any accessibility complaints and requests for accommodation from users with disabilities resulting from Contractor's failure to meet WCAG 2.1 AA guidelines at no cost to the University; and (5) indemnify and hold the University harmless in the event of any claims arising from inaccessibility.

When installation, configuration, integration, updates, or maintenance are provided, the Contractor must ensure these processes are completed in a way that does not reduce the original level of WCAG conformance. If at any point after procurement it is determined that accessibility improvements need to be made in order to comply with the WCAG 2.1 AA standards, the Contractor agrees to work with the University to remedy the non-compliance by submitting a roadmap detailing a plan for improvement on a reasonable timeline. Resolution of reported accessibility issue(s) that may arise should be addressed as high priority, and failure to make satisfactory progress towards compliance with WCAG, as agreed to in the roadmap, shall constitute a breach of contract and be grounds for termination or non-renewal of the agreement.

5. Integration

This DPA applies in addition to, not in lieu of, any other terms and conditions agreed to between Contractor and University, including the Underlying Agreement(s), except as specifically and expressly agreed in writing with explicit reference to these Standards. This DPA governs in the case of any direct conflict with existing terms and conditions in the Underlying Agreement. Any limitations of liability or damages in the Underlying Agreement(s) will not apply to a breach by Contractor of this DPA.

Contractor Acceptance

Contractor Name

Contractor Representative Signature & Printed Name

Date