Northeastern University
Data Processing Addendum: Processor

This Data Processing Addendum ("Addendum") forms part of the agreement ("Principal Agreement") between Northeastern University ("Northeastern", "We", "Us" or "Our") and the service provider ("Service Provider", "You" or "Your") and applies to those services for which We contract with Service Provider ("Services") in a statement of work ("SOW") that include the Processing of Personal Information of individuals. The capitalized terms used in this Addendum shall have the meanings set forth in this Addendum or in the Principal Agreement. In the event of a direct conflict between a specific provision of this Addendum, the Principal Agreement or a SOW, the provision of this Addendum shall prevail.

Processing of Personal Information

For purposes of this Addendum, We are the Data Controller of the Personal Information Processed by Service Provider, and Service Provider is the Data Processor. Service Provider shall Process Personal Information only to perform the Services as specified by Northeastern's documented instructions and in accordance with Applicable Law; in no event shall Service Provider Process Personal Information for any other purpose (including for its own commercial benefit). Supplier will ensure that any of its Affiliates involved in the provision of Services will comply with the terms of this Addendum.

Where the Services involve Service Provider receiving or collecting Personal Information directly from Individuals on Our behalf, Service Provider shall:

- provide any notices and/or obtain consents as required under Applicable Law, and maintain records of such notices and consents or other legal bases relied upon for Processing Personal Information and provide them for review upon Our request
- not use an individual's government identifier as Service Provider's own identifier for that individual

If Service Provider is storing and maintaining Personal Information for Us, Service Provider will:

- keep databases containing Personal Information segregated from other Service Provider Personal Information using logical access restrictions
- promptly update its records with any Personal Information provided by Us or the data subject upon receipt
- log all access to Sensitive Personal Information
- maintain audit trails to detect and respond to Security Incidents, including logging of suspicious events. Such audit trials must be maintained for at least twelve months.

Service Provider Personnel

Service Provider shall limit access to Personal Information to those individuals who need to know or have access to the Personal Information. Such access shall only be granted for the purpose of (i) providing the Services as specified by the Principal Agreement and/or an applicable SOW and in accordance with Applicable Law and (ii) complying with the terms of the Principal Agreement and this Addendum. Service Provider's personnel shall be bound by appropriate confidentiality agreements, be required to take regular data protection trainings, and be required to comply with Service Provider's privacy and security policies and procedures.

Security

Service Provider shall implement and maintain appropriate administrative, technical and organizational measures designed to protect against any misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information that the Service Provider may transmit, store or otherwise Process in its provision of Services to Us. Service Provider shall, at a minimum, implement the security controls set forth in Annex II to the 2021 EU SCCs below.

Sub-processing

Northeastern authorizes Service Provider and its Affiliates to appoint (and each Sub-Processor appointed in accordance with this Section to appoint) Sub-Processors in accordance with the requirements of the Principal Agreement and this Addendum. Service Provider and its Affiliates may continue to use those Sub-Processors already engaged by Service Provider or any Affiliate as at the date of this Addendum, subject to Service Provider and each Affiliate meeting the obligations set out in this Section. Service Provider and each Service Provider Affiliate shall be responsible for each such Sub-Processor's performance of its obligations and compliance with the terms of the Principal Agreement, this Addendum and Applicable Law.

With respect to each Sub-Processor, Service Provider shall:

- before the Sub-Processor begins Processing Personal Information, carry out adequate due diligence to ensure that the Sub-Processor is capable of providing the level of protection for Personal Information required by this Addendum
- ensure that the arrangement between Service Provider and the relevant Sub-Processor is governed by a written contract including terms which offer at least the same level of protection for Personal Information as those set out in this Addendum
- upon request, provide to Us for review such copies of the Contracted Processors' agreements with Sub-Processors (which may be redacted to

remove confidential commercial information not relevant to the requirements of this Addendum)

To the extent that Service Provider Processes Personal Information of residents of the EEA, the UK or Switzerland, the following shall also apply. Service Provider will provide a list of any Sub-Processors prior to the performance of Services and shall give Us prior written notice of the appointment of any new Sub-Processor, including full details of the location and Processing to be undertaken by the Sub-Processor prior to or concurrent with the appointment of such Sub-Processor. If, within 30 (thirty) calendar days' of receipt of that notice, We notify Service Provider in writing of any objections (on reasonable grounds) to the proposed appointment: (i) Service Provider will cancel its plan to use the Sub-Processor for the processing of Northeastern Personal Information and will offer an alternative to provide the Services without such Sub-Processor; or (ii) Service Provider will take the corrective steps requested by Us in its objection(s) and proceed to use the Sub-Processor to process Northeastern Personal Information; or (iii) We may choose not to use the Services that would involve the use of such Sub-Processor with regard to Personal Information, subject to adjustment of the remuneration for the Services considering the reduced scope of the Services. If none of the above options are reasonably available and all of Our objections have not been resolved to the mutual satisfaction of the Parties within 30 (thirty) calendar days of the Service Provider's receipt of Our objection, either Party may terminate the applicable SOW and We will be entitled to a pro-rata refund for prepaid fees for Services not performed as of the date of termination.

Data Subject Rights

Service Provider shall promptly notify Us if any Contracted Processor receives a request from an Individual under Applicable Law with respect to Personal Information and ensure that the Contracted Processor does not respond to that request except on Our documented instructions or as required by Applicable Law, in which case Service Provider shall to the extent permitted by Applicable Law inform Us of that legal requirement before responding to the request.

Upon Northeastern's request, any Contracted Processor shall promptly enable Northeastern to access, rectify, erase, or restrict Personal Information from further Processing or request a portable copy.

Security Incident Response

Service Provider shall implement and maintain appropriate measures designed to detect, analyze, monitor and resolve Security Incidents, and will notify Us promptly and without undue delay upon Service Provider or any Contracted Processor becoming aware of a Security Incident, providing Us with sufficient information to allow it to meet any obligations to report or inform Individuals of the Security Incident under Applicable Law. Such notification shall as a minimum:

- describe the nature of the Security Incident, the categories and numbers of Individuals concerned, and the categories and numbers of Personal Information or other data records concerned
- communicate the name and contact details of Service Provider's data protection officer or other relevant contact from whom more information may be obtained
- describe the likely consequences of the Security Incident
- describe the measures taken or proposed to be taken to minimize the impact of such Security Incident and prevent such events from recurring

Service Provider shall assist in the investigation, mitigation and remediation of the Security Incident. Unless otherwise required by law, Service Provider shall not notify any Supervisory Authority or affected Individuals or issue any public notice of any Security Incident that could directly or indirectly identify Us without Our prior written consent.

Service Provider Cooperation and Assistance

Service Provider shall provide reasonable assistance to Northeastern with any data protection impact assessments, security questionnaires, customer inquiries, and consultations with competent Supervisory Authorities or other competent data privacy authorities related to the Processing of Personal Information under this Addendum.

Unless prohibited by Applicable Law, Service Provider shall promptly notify Us prior to taking any action and coordinate with Us in the event that Service Provider receives:

- a request for Personal Information from a law enforcement agency, state security agency, or other similar governmental body
- a request by a Supervisory Authority for information concerning the Processing of Personal Information
- a complaint or inquiry by an Individual related to Service Provider's Processing of Personal Information

In the event Service Provider Processes Personal Information that is subject to additional regulatory requirements or in a manner subject to additional regulatory requirements (including those requirements imposed with respect to Sensitive Personal Information), Service Provider agrees to cooperate with Us to comply with such requirements, including without limitation negotiating in good faith any required amendments to the Principal Agreement and/or this Addendum.

Service Provider will promptly inform Us if Service Provider has reason to believe that (i) it is or may become unable to comply with the obligations of this Addendum or Applicable Law; or (ii) Our instructions regarding the Processing of Personal Information would violate Applicable Law. Service Provider and each Service Provider Affiliate shall promptly take adequate steps to remedy any noncompliance with this Addendum or Applicable Law regarding the Processing of Personal Information by any Contracted Processor. We have the right to suspend or temporarily restrict any impacted Processing under the Principal Agreement until such noncompliance is remediated. In the event such remediation is impossible or unduly delayed, We may terminate the Services immediately, in whole or in part.

Deletion or Return of Personal Information

Except to the extent otherwise required by Applicable Law, Service Provider shall promptly and securely return in a mutually-agreed format or delete all copies of Personal Information upon cessation of the applicable Services or upon Our request. Deletion must be performed in a manner designed to ensure the data may not be recovered and Service Provider shall provide Us written confirmation of its compliance with this provision upon request.

Compliance Reviews

No more than once per year, Service Provider shall make available to Us upon request information reasonably necessary to confirm compliance with this Addendum and Applicable Law. Such information may not compromise any confidentiality obligations Service Provider may have to its customers. At Our request, Service Provider will also provide a copy of its most recent third-party assessment(s), such as an SSAE SOC 2, ISO 27001 or similar. Service Provider agrees to support a live review of its compliance with this Addendum and Applicable Law in the event that:

- We have received evidence that Service Provider or its Affiliate is in breach of its obligations
- Service Provider or its Affiliate experiences a Security Incident
- Northeastern or its Affiliate is required or requested by a Supervisory Authority or similar regulatory authority

International Transfers of Personal Information

International Transfers of Personal Information. To the extent that the Services involve an International Transfer of Personal Information from Northeastern or its Affiliate(s) to Service Provider, a Service Provider Affiliate or a Sub-Processor, the International Transfer shall be subject to the terms of this Addendum. If additional terms are required to meet the requirements for International Transfers from a specific jurisdiction, the Parties agree to negotiate in good faith to amend this Addendum to include the required terms.

International Transfers from the EEA, Switzerland and UK. To the extent that the Services involve the International Transfer of Personal Information of a resident(s) of a country within the European Economic Area ("EEA"), Switzerland or United Kingdom ("UK") to Service Provider, a Service Provider Affiliate or a Sub-Processor located outside of the EEA, Switzerland or UK and the International Transfer is not covered by a European Commission Adequacy Decision and there is not another legitimate basis for the International Transfer of such Personal Information, then such transfers are subject to either the 2021 EU Standard Contractual Clauses, the UK SCC Addendum and/or Swiss SCC Addendum (as applicable) or other valid transfer mechanisms available under Applicable Law. For International Transfers subject to:

- the GDPR, the Parties hereby incorporate the 2021 EU SCCs in unmodified form (Module Two: Controller to Processor).
- the UK Data Protection Laws, the Parties hereby incorporate by reference the UK SCC Addendum in unmodified form.
- The FADP, the Parties hereby incorporate by reference the Swiss SCC Addendum.

The 2021 EU Standard Contractual Clauses shall be between Service Provider and Northeastern. For such purposes, We will act as the "data exporter" on its behalf and/or on behalf of its Affiliates, and Service Provider will act as the "data importer" on its behalf and/or on behalf of its Affiliates. With respect to the 2021 EU SCCs, the Parties agree to the following: (i) Clause 7 shall be omitted; (ii) Clause 9 shall be governed by Option 2 (General Authorization) and provide for a 14-day advance notice; and (iii) for Clauses 17 and 18, the Parties choose Ireland and the Supervisory Authority of Ireland.

For purposes of the UK SCC Addendum, the Parties (i) select the Approved EU SCCs, including the Appendix, in Table II and (ii) select both Importer and Exporter in Table 4. Annexes I and II of the 2021 EU SCCs are attached hereto and shall serve to provide the information required for Table 1 of the UK SCC Addendum.

For the purposes of the Swiss SCC Addendum, (i) the term "member state" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the 2021 EU SCCs; (ii) the references to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP; (iii) the Federal Data Protection and Information Commissioner of Switzerland shall be the competent supervisory authority in Annex I.C under Clause 13 of the 2021 EU SCCs, where the transfer of Personal Information is subject to the FADP.

In the event of any direct conflict between this Addendum and the 2021 EU Standard Contractual Clauses, the UK SCC Addendum and/or Swiss SCC Addendum the 2021 EU Standard Contractual Clauses, the UK SCC Addendum and/or the Swiss SCC Addendum (as applicable) shall prevail.

Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly.

"Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with the relevant party.

"**Applicable Law**" means any applicable law, statute, regulation, directive, order or other binding restriction (including any amendments or successors thereto) to which Service Provider and Northeastern (and their Affiliates) are subject and which is applicable to Service Provider's or Northeastern's privacy or data protection obligations related to the Services (including without limitation the US Family Education Rights & Privacy Act, GDPR and UK Data Protection Laws).

"**Contracted Processor**" means Service Provider, Affiliate or a Sub-Processor.

"**GDPR**" means EU General Data Protection Regulation 2016/679/EU.

"**Individual**" means any identified or identifiable individual about whom Personal Information may be Processed under the Principal Agreement.

"**International Transfer**" means the access, transfer, delivery, or disclosure of Personal Information to a person, entity or computing system located in a country other than the country from which the Personal Information originated.

"**2021 EU Standard Contractual Clauses**" or "**2021 EU SCCs**" mean the contractual clauses annexed to the EU Commission Decision 2021/914/EU or any successor clauses approved by the EU Commission.

"**Personal Information**" means any information Processed in connection with the performance of Services (including without limitation the information of Northeastern and its students, employees, alumnae/I, customers, partners, vendors, contractors and service providers) that can identify a unique individual, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of individuals or as such information may be otherwise defined under Applicable Law.

"**Security Incident**" means the unauthorized access to or Processing of Personal Information that compromises the confidentiality, integrity, or availability of the information.

"**Sub-Processor**" means any person (including any third party and any Service Provider Affiliate, but excluding an employee of Service Provider or any of its sub- contractors) appointed by or on behalf of Service Provider or any Service Provider Affiliate to Process Personal Information on behalf of Northeastern or its Affiliates in connection with the performance of Services.

"**Swiss SCC Addendum**" means adaptation of the 2021 EU SCCs to comply with the Swiss legislation in order to ensure an adequate level of protection for data transfers from Switzerland to a third country subject to the Swiss Federal Act on Data Protection ("**FADP**").

"**UK Data Protection Laws**" means the UK GDPR and the Data Protection Act 2018, or any successor UK data protection laws as updated, amended or replaced from time to time.

"**UK SCC Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (vB1.0 or any subsequent version) issued by the UK Information Commissioner's Office.

The terms, "**Commission**", "**Controller**", "**Member State**", "**Processor**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as under Applicable Law (e.g., the GDPR) (except in the context of Module Three of the New EU SCCs when "Controller" as used herein is a Data Exporter acting as a Processor, in which case Processor shall mean Sub-Processor).

2021 EU SCC ANNEXES

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Northeastern University

The contact information, signature and date provided in the Principal Agreement are incorporated herein by reference

Activities relevant to the data transferred under these Clauses: Receiving products, services and solutions as described in Principal Agreement.

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Service Provider

The contact information, signature and date provided in the Principal Agreement are incorporated herein by reference

Activities relevant to the data transferred under these Clauses: Providing products, services and solutions as described in Principal Agreement. Role

(controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As needed in order for Service Provider to perform the Services, which may include:

- Employees
- Students, their parents/guardians and Alumnae/i
- Applicants (both student and employee)
- Researchers, Customers and end users
- Service providers, agents, and contractors

Categories of personal data transferred

As needed in order for Service Provider to perform the Services, which may include:

- Direct identifiers such as first name, last name, date of birth, and home address
- Education records and information, including transcript, student ID, loans, visa applications, health and discipline records
- Communications data such as home telephone number, cell telephone number, email address, postal mail, and fax number
- Family and other personal circumstance information such as age, date of birth, marital status, spouse/ partner, and number & names of children
- Employment information such as employer, work address, work email and phone, job title and function, salary, manager, employment ID, system usernames and passwords, performance information, and CV data
- Other data such as financial, goods or services purchased, device identifiers, online profiles, and IP address
- Details of user's interaction with the data importer's systems and with systems for which the data importer provides computing services
- Information that the data exporter or its users choose to include in files stored on or routed through data importer's applications
- Other Personal Information to which the Parties provide to each other in connection with the provision of Products or Services

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Personal data transferred is determined and controlled by the data exporter and may include sensitive data such as government identifier, health information, religious affiliation, or any other sensitive data necessary to be Processed in order to perform the Services.

Technical and organizational security measures are described in Annex II below.

The frequency of the transfer *(e.g., whether the data is transferred on a one-off or continuous basis).*

Transfers on a continuous basis as needed to perform the Services.

Nature of the processing

Please refer to Section 1 of the Addendum.

Purpose(s) of the data transfer and further processing

Please refer to Section 1 of the Addendum.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Retained for the duration of the Services.

For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing

Transfers on a continuous basis as needed to perform the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in an EU Member State: Supervisory Authority of Ireland.

Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: Supervisory Authority of Ireland.

Where the data exporter is not established in an EU Member State but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: Supervisory Authority of Ireland.

ANNEX II

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

Service Provider agrees to use reasonable and appropriate physical, technical and administrative measures to safeguard the data received from Northeastern against any misuse or accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access. Such measures shall include, at a minimum:

- Limiting access to authorized users based on role and least-privilege
- Prompt removal of system access at the end of employment
- Publishing, maintaining and enforcing written information security policies (including system use, data classification and incident response)
- Implementing security processes for managing vendors and contractors throughout the business relationship lifecycle
- Performing security assessments, scans and testing of systems, networks and applications at regular intervals (at least annually) to verify compliance with organizational security policies and standards
- Following change management procedures for controlling configuration changes to systems, applications and network devices
- Maintaining firewalls, intrusion detection/prevention systems (IDS/IPS) and other network security infrastructure tools to detect, monitor and restrict network traffic flow
- Maintaining security logs from systems, network devices and applications for a minimum of 90 days
- Promptly applying patches for all operating systems, applications and network devices
- Using anti-virus/malware detection software to prevent, detect and remove malicious code
- Enforcing strong password practices, including minimum password length and complexity requirements
- Ensuring no Northeastern data is stored on a laptop computer, mobile device or device media card unless it is encrypted using 256-bit or higher encryption
- Implementing and maintaining a physical security plan to protect offices and information processing facilities from internal and external threats of unauthorized access, including use of access cards and keys to limit access to secure areas
- Implementing a comprehensive security awareness program for all personnel that encompasses education, training and updates