

## **Northeastern University**

### **Data Processing Addendum: Controller**

This Data Processing Addendum ("Addendum") forms part of the agreement ("Principal Agreement") between Northeastern University ("Northeastern", "We", "Us" or "Our") and the or other party to the Principal Agreement ("You" or "Your") and applies to those services for which We contract with You ("Services") as part of the Principal Agreement and/or 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**

The parties acknowledge that each shall be responsible for the Processing of Personal Information under its control for the purposes specified in the Principal Agreement and pursuant to the terms of this Addendum, and not for any other purpose unless You obtain Northeastern's or the individual's prior consent for such Processing activities. Each party shall comply with its obligations as a Data Controller under Applicable Law. You will regularly review the Processing of Personal Information under the Principal Agreement for compliance with Applicable Law. Unless specified in the Agreement, neither party will provide the other with access to any Personal Information that imposes specific data protection requirements greater than those agreed to in the Principal Agreement or this Addendum, and each party will limit the other party's access to Personal Information as necessary to accomplish the purposes set forth in the Principal Agreement. Neither party will take measures to Re-Identify any of the other party's Personal Information unless otherwise agreed in a SOW.

Where the Services involve You receiving or collecting Personal Information directly from Individuals on Our behalf, You 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 Your own identifier for that individual

If You are storing and maintaining Personal Information for Us, You will:

- keep databases containing Personal Information segregated from Your other 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 trails must be maintained for at least twelve months.

#### **Security**

You 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 You may transmit, store or otherwise Process in its provision of Services to Us. You shall, at a minimum, implement the security controls set forth in Annex II to the 2021 EU SCCs below.

#### **Processing by a Third Party**

You will not permit the Processing of Personal Information in connection with the Services by any third party unless they have, prior to receiving access to such Personal Information, entered into an agreement with You with terms at least as restrictive as those contained herein. You will be responsible for such third parties' compliance with the terms of the Principal Agreement and this Addendum.

#### **Data Subject Rights**

Each party shall, at its own cost, provide reasonable assistance to the other party in the event of a Data Subject request or other inquiry (including the request to correct, delete, release and/or block Personal information from further Processing). The parties will cooperate to the extent necessary with respect to any action that must be taken related to such request and will identify a contract personal authorized to respond to assist with Controller obligations under this Addendum within a reasonable time.

#### **Security Incident Response**

You 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 You any third party you engage to assist in the provision of Services becoming aware of a Security Incident, providing Us with sufficient information to determine whether any such Security Incident may impact the security of the Services.

#### **Cooperation and Assistance**

You 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, You 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 Your Processing of Personal Information

In the event You 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), You agree 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.

Each party will promptly inform the other if it has reason to believe that it is or may become unable to comply with the obligations of this Addendum or Applicable Law and shall promptly take adequate steps to remedy any noncompliance with this Addendum or Applicable Law . 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.

## **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 You, one of Your Affiliates or a third party you use to provide the Services, 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 You, one of Your Affiliates or a third party You use to provide the Services 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 One: Controller to Controller).
- 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 You and Northeastern. With respect to the 2021 EU SCCs, the Parties agree to the following: (i) Clause 7 shall be omitted; and (ii) Clause 11 option shall be omitted; 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 Data 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 You and Northeastern (and their Affiliates) are subject and which is applicable to Your 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).

**"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/l, 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.

**"Re-Identify"** means any process whereby the receiving party adds data to the Personal Information supplied by the providing party related to an individual in a manner that could be used to or does identify that individual.

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

**"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 & You (depending on the Services)**

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 or providing (as applicable) 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]*

**You & Northeastern (depending on the Services)**

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 or providing products, services and solutions as described in Principal Agreement. Role (controller/processor): Controller

#### B. DESCRIPTION OF TRANSFER

***Categories of data subjects whose personal data is transferred***

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

- Direct identifiers such as first name, last name, date of birth, and home address
- Student 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, 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**

Each party agrees to use reasonable and appropriate physical, technical and administrative measures to safeguard the data received from the other party 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 data received from the other party 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
- Implementing a comprehensive security awareness program for all personnel that encompasses education, training and updates