[Rider dated as of March 1, 2021, concerning requirements relating to data processing under the EU's General Data Protection Regulation ("GDPR") or the Data Protection Act 2018 of the United Kingdom (the "Act"). This Rider is for contracts with vendors who, on behalf of any Harvard unit, will process personal data relating to identified or identifiable individuals located in the European Economic Area (the EU plus Iceland, Norway and Liechtenstein) or in the United Kingdom.

The United Kingdom has adopted national legislation implementing the GDPR, namely, the Data Protection Act 2018. As of its transition out of the EU (effective January 1, 2021), the United Kingdom is no longer technically subject to the GDPR. However, this UK legislation will remain in place and UK authorities have indicated they intend to follow GDPR principles as applied in the EU.

EU members are listed here: https://europa.eu/european-union/about-eu/countries/member-countries_en .

"Processing" and "Personal Data" are defined below.

This Rider or equivalent terms should be used in contracts with vendors who process data about individuals in the EEA or in the UK, usually in connection with Harvard offering or providing goods or services to such individuals, for example, employees, alumni, students in EEA-based or UK-based programs, and online course participants located in the EEA or the UK. If vendors are engaged to monitor individuals in the EEA or the UK, such contracts should also include this Rider or equivalent terms. These terms do not need to be used with vendors who, with only incidental exceptions, process data relating to activities of individuals while they are in the US, or relating to Harvard services provided to such individuals in the US.

In some cases, a vendor contract that includes this Rider may also require the attachment of the Rider on Requirements for the Protection of Harvard Personally Identifiable Information, the Rider for the Protection of Credit Card Data, or both.

Material changes in this form must be approved by the Harvard Office of Strategic Procurement or by the Office of the General Counsel.

Indemnification: when possible, it is preferable to cover indemnification arising in connection with this Rider, and related limitation of liability when applicable, in the underlying contract in conjunction with indemnification of other confidentiality/data protection claims. It will need to be expressly stated that such underlying contract terms apply to the Rider, if that is the desired result. For that reason, if this Rider is being added to an existing agreement it may also be necessary to amend the indemnification and limitation of liability terms in the existing agreement. Alternatively, in some cases the "default" provision in this Rider set out as Section 13 will be needed or preferable, for example, if the underlying agreement does not contain a suitable indemnification provision or the vendor will not agree to extending an existing provision to this Rider. Section 13 should be deleted if it does not apply.

Please discuss questions about this form with the Office of Strategic Procurement or the Office of the General Counsel and consult with them if the vendor rejects this Rider or insists on use of the Vendor's own GDPR language.

Please delete this headnote and any instructions from this Rider before transmitting.]

Rider:
Requirements for the Protection of Personal Data under the European Union General Data Protection Regulation or the United Kingdom Data Protection Act 2018

Effective as of _____, this Rider (the "**Rider**") is added to and incorporated as part of the *[name of Agreement]* (in this Rider, the "**Agreement**"), dated as of _____, between *[identify Harvard party]* (in this Rider, "**Harvard**") and *[identify service provider/vendor]* (in this Rider, "**Service Provider"**).

This Rider applies to Processing subject to applicable Referenced Law when Personal Data is being processed by the Service Provider, as Processor, for Harvard, as Controller, all as defined herein.

1. DEFINITIONS

Capitalized terms used but not defined in this Rider will have the meanings set forth in the Agreement. The following words and expressions shall have the following meanings:

"Controller" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data under the Agreement or this Rider.
"**Data**" means all Personal Data processed by the Service Provider or a Subprocessor for Harvard as the Controller under or in connection with the Agreement, including in connection with the provision of the Services;
"Data Subject" means an identified or identifiable natural person;
"**Data Subjects' Rights**" means the rights of Data Subjects set out in applicable Referenced Law including, without limitation, rights of access, rectification, erasure, restriction of Processing, data portability, objection, and not to be subject to automated decision making (including profiling);

"Personal Data" means any information relating to a Data Subject;
"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, Personal Data;
"Processing" (and "process") means any operation or set of operations subject to applicable Referenced Law 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;
"Processor" means the party which processes Personal Data on behalf of the Controller.
"Referenced Law" means either (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of personal data (the **"GDPR"**), or (ii) the United Kingdom Data Protection Act 2018 (the **"Act"**).

"Services" means the services, work, tasks, or other activities, including Processing, that the Service Provider will perform for Harvard as described in the Agreement;
and
"**Subprocessor**" means any third party: (i) who is engaged by the Service Provider to carry out specific Processing activities in respect of the Data for or on behalf of Harvard as the Controller under the Agreement; or (ii) to whom the Service Provider subcontracts any of its Processing obligations under or in connection with the Agreement.

2. SCOPE OF PROCESSING

The duration of Processing will be the same as the term of the Agreement, except as otherwise agreed to in the Agreement or in writing by the Parties. The scope and further details of the Processing activities to be performed by the Service Provider under or in connection with the Agreement are set out in the Agreement and in Schedule I of this Rider if applicable.

3. GENERAL SERVICE PROVIDER OBLIGATIONS

The Service Provider shall:

3.1 only process Data (i) as is necessary for the provision of the Services and not for its own purposes or for any other purposes, (ii) in accordance with the terms of this Rider, and (iii) in accordance with the written instructions of Harvard from time to time, unless otherwise required by applicable law (provided that in any such case, the Service Provider shall promptly inform Harvard of the relevant legal requirement before Processing, unless prohibited by law from doing so);

3.2 keep Data confidential; and

3.3 on request from Harvard, from time to time provide an up-to-date copy of all Data in any commonly available format and media and within any reasonable time periods required by Harvard.

In carrying out its obligations under the Agreement (including, in particular, in the provision of the Services), the Service Provider shall comply in full with all applicable laws, regulations and codes of practice relating to privacy or data protection, including, without limitation, applicable Referenced Law.

The Service Provider shall also require each of its employees and any other individuals acting under its authority who have access to the Data to comply with the provisions of this Section 3.

4. SECURITY

In connection with its Processing of Data under or in connection with the Agreement, the Service Provider shall implement appropriate technical and organizational security measures appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing, as well as the specific risks of varying likelihood

and severity that may be presented by the Processing for the rights and freedoms of natural persons, especially as a result of accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to the Data.

5. SUBPROCESSORS

5.1 The Service Provider shall not engage any Subprocessor, or otherwise subcontract any of its obligations under or in connection with the Agreement, without the prior specific written approval of Harvard in each case, except as authorized in the Agreement.

5.2 The Service Provider shall ensure that all the data protection obligations set out in this Rider are imposed on such Subprocessor by way of a written agreement, and in particular (but without limitation) shall require each Subprocessor to implement appropriate technical and organizational measures in such a way that Processing by the Subprocessor will meet the requirements of applicable Referenced Law. The Service Provider shall remain fully liable to Harvard for the performance of any Subprocessor's obligations, including all data protection obligations.

6. RIGHTS OF DATA SUBJECTS; OTHER ASSISTANCE

6.1 Taking into account the nature of the Processing performed by the Service Provider, the Service Provider shall assist Harvard by appropriate technical and organizational measures, insofar as this is possible, in the fulfillment of Harvard's obligations to respond to requests for exercising Data Subjects' Rights.

6.2 The Service Provider shall notify Harvard in writing of each such request that it receives from Data Subjects. Such written notification shall be made promptly and, in any event, not later than three (3) working days following receipt of the request and shall include any information in the Service Provider's custody or control that may assist Harvard to respond to the request. Such written notification shall identify the Agreement and this Rider and shall be sent both (i) as required for notices under the Agreement, and (ii) to eeadatasubjectrequest@harvard.edu.

6.3 Unless otherwise required by applicable law, the Service Provider shall not respond to any such requests or other communications which the Service Provider receives from Data Subjects, without the prior written consent of and at the direction of Harvard.

6.4 The Service Provider shall, at its expense and to the extent applicable to the Service Provider, also assist Harvard to comply with the obligations set forth by applicable Referenced Law regarding security of Processing and data protection impact assessments.

7. DATA BREACHES

The Service Provider shall notify Harvard in writing without undue delay after becoming aware of any Personal Data Breach in any way relating to or affecting the Data. Such notification shall include the nature of the data breach, including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Data records

concerned. Such written notification shall identify the Agreement and this Rider and shall be sent both (i) as required for notices under the Agreement and (ii) by email to the Service Provider's then-current primary contact person at Harvard. The Service Provider shall at the Service Provider's expense reasonably cooperate with Harvard in the remediation of such event, including without limitation, at Harvard's request providing reasonable assistance with notification of any Personal Data Breach that Harvard decides to make to the relevant supervisory authority or to the Data Subjects.

8. INTERNATIONAL TRANSFERS OF DATA

The Service Provider shall not transfer any Data to any third country or international organization outside the European Economic Area or the United Kingdom except as provided in the Agreement or on the written instructions or with the prior written approval of Harvard.

9. OTHER DATA PROTECTION REQUIREMENTS; ORDER OF PRECEDENCE

The Service Provider shall also comply with all other data protection and confidentiality obligations set out in the Agreement. This Rider supplements, and does not replace, any other obligations related to the confidentiality, security and protection of Personal Data set forth in the Agreement. Subject to the preceding sentence, in the event of a conflict between the terms of this Rider and the Agreement, the terms of this Rider will govern.

10. ACCOUNTABILITY

10.1 Upon reasonable written notice from Harvard, the Service Provider shall make available to Harvard all information reasonably required to demonstrate compliance with any or all of the Service Provider's obligations under this Rider and shall permit and cooperate with audits, including inspections, by Harvard or Harvard's agent pertinent to such compliance. The Service Provider shall also require each Subprocessor to comply with this audit provision.

10.2 The Service Provider shall immediately inform Harvard if, in the Service Provider's opinion, any instruction from Harvard with respect to the Processing of Data under or in connection with the Agreement including this Rider infringes applicable Referenced Law or other applicable data protection law or regulation.

10.3 The Service Provider shall notify Harvard of all communications it receives from any third party relating to the Data which suggest non-compliance by Harvard, the Service Provider or any other person with applicable Referenced Law or any other law or regulation relating to the privacy or protection of Personal Data, including any such communications from Data Subjects and regulatory bodies, and shall not respond to such third party or take any other action with respect to such communications unless expressly authorised to do so by Harvard. The Service Provider's written notification shall identify the Agreement and this Rider and shall be sent both (i) as required for notices under the Agreement and (ii) by email to the Service Provider's then-current primary contact person at Harvard.

10.4 The Service Provider shall maintain (or procure the maintenance of) all records required by applicable Referenced Law, including a written record (which can be in electronic form) of all categories of Processing activities carried out by the Service Provider on behalf of Harvard, containing those details specified in Article 30 of the GDPR or the equivalent provisions of the Act, and the Service Provider shall make those records available to Harvard on Harvard's request.

11. RETURN OR DISPOSAL

Upon completion of the Services or upon the expiry or termination of the Agreement for any reason, and in any event on the written request of Harvard, the Service Provider shall (and shall procure that any permitted Subprocessor shall), at Harvard's discretion: (i) return all Data processed under or in connection with the Agreement (including any and all copies thereof) to Harvard or to any other person as directed by Harvard in writing; and (ii) securely delete or destroy all such Data remaining in Service Provider's possession so that the Data thereafter cannot practicably be accessed or reconstructed. If the Service Provider believes that it cannot comply with the foregoing destruction requirement because any applicable law requires the retention of such Data, the Service Provider shall promptly inform Harvard of such requirement.

12. SURVIVAL

The obligations in this Rider shall continue for so long as any Data remains in the Service Provider's custody or control, or the Service Provider (or any permitted Subprocessor) continues to process Data under or in connection with the Agreement, notwithstanding the termination of the Agreement for any reason.

13. INDEMNIFICATION

The Service Provider shall indemnify and hold Harvard and its affiliates, employees, faculty members, students, fellows, members of its governing boards and agents harmless from and against any claims, losses, liabilities, damages, costs and expenses including reasonable attorneys' fees arising out of or relating to the Service Provider's breach or alleged breach of any provision of this Rider or of applicable Referenced Law. This paragraph shall apply without regard to any contrary provision (including any limitation of liability) in the Agreement. Neither party will enter into any settlement that admits fault on the part of the other or requires any payment, commitment or action from the other without the other's written consent.

For Service Provider	**For Harvard**
By_____	By_____
Name:	Name:
Title:	Title:

[Under applicable Referenced Law, this Rider or the Agreement must contain descriptions of (a) the business purposes of the vendor's data processing for Harvard;(b) the types of data the vendor will process; and (c) the categories of data subjects affected. If this information is stated in or clear from the Agreement or a Statement of Work, Schedule I will not be needed and should be marked as not applicable in the box provided. Otherwise, this information should be set out in Schedule I. If Schedule I applies:

- *Clause A: Default language is provided below which should be modified as appropriate*
- *Clause B: It is sufficient to state types of data generically in the Agreement or this Schedule if this makes the scope of the processing reasonably clear. For example, name, address, email address etc. may be described as "contact information" and name, salary, etc. may be described as "employment records"; however, "all personal data provided to the Service Provider" would not be adequate. Any special categories of data under Referenced Law that are to be processed should be specified if that processing is a main purpose of the contract. The special categories include: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, 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.*
- *Clause C: Complete as appropriate; again, generic descriptions, for example, students, alumni, employees, etc., may be used.]*

☐ CHECK BOX IF SCHEDULE I IS NOT APPLICABLE

SCHEDULE I
SCOPE OF PROCESSING

A. PURPOSE OF PROCESSING
The Processing is being conducted as needed to perform the Services.

B. DATA TO BE PROCESSED
The types of Data to be processed by the Service Provider include the following categories of Personal Data:

C. DATA SUBJECTS
The Data to be processed by the Service Provider relates to the following categories of Data Subjects: