**UNIVERSITY OF WASHINGTON**

**CONTROLLER TO PROCESSOR**

**DATA PROCESSING AGREEMENT**

# Introduction, Parties, AND Effective Date

This Data Processing Agreement (the “DPA”) is hereby incorporated into and amends the [insert name of Underlying Agreement] (the “Agreement”) between the University of Washington, an agency of the State of Washington, with its main campus located in Seattle, Washington (the “University”) and [insert entity name], a [insert name of jurisdiction within which entity was formed (ex. Delaware)] [insert type of entity type (ex. corporation)], with a principal place of business at [insert entity’s address] as of the Effective Date below. With respect to Data Processing performed under the Agreement and this DPA, the University is the Controller and the [insert non-UW entity] is the Processor. The parties agree as follows:

# Definitions

1. **“Controller”** refers to the person or entity that determines the purpose and means for Data Processing.
2. “**Data Breach**” means any technical or physical incident or set of circumstances that leads to the unauthorized, accidental or unlawful access to, or destruction, loss, alteration, or disclosure of, University Personal Data undergoing Data Processing by the Processor.
3. “**Data Processing**” means any operation(s) performed on University Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, access, use, disclosure by transmission, dissemination, combination, restriction or destruction.
4. **"Data Request”** means a request to exercise rights available under any applicable law with respect to University Personal Data.
5. **“Processor”** refers to the person or entity that performs Data Processing on behalf of the Controller.
6. “**Sub-processor**” means any person or entity appointed by or on behalf of the Processor to carry out any portion of the Work.
7. “**University Personal Data**” **or “UPD”** means any records or information relating to an identified or identifiable natural person, such as name, identification number, location data, online identifiers, or factor(s) specific to physical, physiological, genetic, mental, economic, cultural, or social identity or characteristics, or is identified as personally identifiable data (or a similar term) by any applicable law, that:
	1. Is created, received, or maintained by the University and transmitted to, accessed by, or otherwise made available to the Processor in connection with the Processor’s performance of the Work;
	2. Is created or compiled by the Processor in performing the Work; or
	3. Is appended to, aggregated with, or associated with any University Personal Data originating from the University that was transmitted to or accessed by the Processor in connection with the Processor’s performance of the Work.

Notwithstanding the foregoing, UPD does not include personal data relating to the Processor’s or Sub- processor’s personnel or personal data that is acquired from non-UW sources and is processed by the Processor not in association with the Work.

1. “**Processor**” as used in this DPA includes both the Processor identified above, and any third party and/or entity that owns or controls, is owned or controlled by, or is under common ownership or control with the Processor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting security, by contract, or otherwise.
2. “**Work**” refers to any and all activities carried out by the Processor or a Sub-processor in providing services, work product or deliverables under the Agreement, or in fulfilling any other obligations set forth in the Agreement.

# standard of care

* 1. The Processor represents and warrants that any Data Processing shall be by personnel who (a) are obligated to maintain confidentiality under applicable law or job expectations, and (b) are sufficiently trained and experienced to use reasonable care commensurate with state-of-the-art professional practices to comply with the obligations in this DPA.
	2. The Processor shall ensure that there are appropriate personnel-vetting processes, and appropriate policies and/or controls over activities as necessary to safeguard UPD per this DPA and applicable law.
	3. Prior to the disclosure of UPD to, or the commencement of Data Processing by any Sub-processor, the Processor shall cause each Sub-processor to execute an agreement with the Processor that includes terms and conditions which establish at least the same level of protection for UPD as those set out in this DPA and applicable law. If a Sub-processor fails to fulfill its data protection obligations under this DPA or applicable law, the Processor shall remain fully liable to the University for the performance of that Sub-processor’s obligations.

# purpose And LIMITS OF DATA PROCESSING

1. The Description of Data Processing Exhibit to this DPA sets forth certain information relating to the Data Processing by the Processor for the purpose of carrying out the Work. The Processor may only engage in Data Processing for the limited purpose described in the Description of Data Processing Exhibit (the “Purpose”). The Processor shall limit its Data Processing to include only the minimum UPD needed to fulfill the Purpose. The Processor’s Data Processing will not involve any secondary uses of UPD beyond the Purpose. Without limiting the generality of the foregoing, the Processor shall not use any UPD to market or sell goods or services to persons named or otherwise identified in UPD.
2. When the University reasonably deems necessary to meet its own requirements and/or applicable laws, the University may make reasonable changes to the Data Processing by amending the Description of Data Processing Exhibit or providing the Processor with an additional exhibit in the same form as the Description of Data Processing Exhibit. Any material change to the Description of Data Processing Exhibit that increases the cost of the Work shall be subject to the mutual agreement of the parties.
3. The University shall have sole control over determinations related to (a) the lawfulness of the Data Processing, and (b) the necessity of any privacy notice to and/or solicitation of consent from individuals whose personal data will undergo Data Processing in relation to the Work.

# Non-Disclosure AND DATA REQUESTS

1. UPD shall not be disclosed by the Processor (or any Sub-processor) to a third party, unless the University grants permission in writing to the Processor to disclose, or unless such disclosure is required by applicable law.
2. If the Processor receives any subpoena, discovery request, court order, or other legal request or order that calls for disclosure of any UPD, then the Processor shall promptly notify the University unless specifically prohibited by law from doing so. The Processor’s notification shall give the University sufficient time to object to the disclosure, obtain a protective order, or otherwise protect UPD by limiting disclosure. The Processor shall provide the University with prompt and full assistance in the University’s efforts to protect UPD. Any disclosure pursuant to this section shall be limited to the minimum disclosure required by law.
3. The Processor shall assist the University by implementing technical and organizational measures, to the extent practicable, in order for the University to meet its obligations (as understood by the University) to respond to Data Requests relating to UPD held by the Processor. The Processor shall promptly notify the University if the Processor receives a Data Request, assist the University in the University’s response, and respond to the Data Request directly only on the documented instructions of the University or as required by applicable laws to which the Processor is subject, in which case the Processor shall, to the extent permitted by applicable laws, inform the University of the Processor’s legal obligations before any response to the Data Request.

# Compliance and Data Transfers

1. The Processor shall conduct all Work and Data Processing in full compliance with any and all applicable statutes, regulations, rules, standards and orders of any official body with jurisdiction over the Processor or the University. Applicable statutes, regulations, rules, or orders may include, but are not necessarily limited to:
	1. The Family Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. §1232g; 34 CFR Part 99;
	2. The Health Insurance Portability and Accountability Act (“HIPAA”), 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq.; and/or the Washington Health Care Information Act, Ch. 70.02 RCW; and
	3. European Union General Protection Data Regulation (“GDPR”), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. The University’s obligations and rights with respect to GDPR are set forth in the Agreement and this DPA. The Agreement, this DPA, and any directions contained in notices from the University to the Processor pursuant to § J.4 together constitute the University’s documented instructions to the Processor for the purposes of GDPR. The subject matter of the Data Processing with respect to GDPR is the Work, as defined above, in the Agreement, and/or in the Description of Data Processing Exhibit to this DPA (including any change(s) pursuant to § D.1). Compliance with GDPR includes, without limitation, the following:
2. The Processor shall provide the University with assistance and information required by GDPR, to the extent applicable, as it relates to Data Processing. As contemplated by GDPR, the Processor’s provision of assistance may relate to data protection impact assessments, prior consultations, demonstration of compliance with Article 28 of GDPR, and audits. The Processor will also immediately notify the University if, in its opinion, a University instruction infringes GDPR.
3. The Sub-processors that are identified and described by the Processor in the Description of Data Processing Exhibit of this DPA are the only Sub-processors permitted to perform Data Processing. Prior to engaging a new Sub-processor for Data Processing, the Processor shall: (1) notify the University in writing of the intended addition or replacement of the Sub-processor; and (2) give the University the opportunity to object to such change.
4. For Data Processing that involves transfers of UPD from the European Economic Area, Switzerland, or the United Kingdom to a country that does not ensure an adequate level of data protection (including, but not limited to, the United States) within the meaning of the applicable laws of the foregoing territories, the Standard Contractual Clauses (accessible at <https://privacy.uw.edu/design/agreements/dpa/> shall govern such transfers.

# SAFEGUARDING DATA

1. Taking into consideration the state of the art, costs of implementation and the nature, scope, context and purposes of the Data Processing, the likelihood and potential severity of risks to the rights and freedoms of natural persons, and the risk of Data Breach, the Processor represents and warrants that it shall implement technical, physical, and administrative security measures appropriate to such risks, which may include, but are not necessarily limited to:
	1. The de-identification, anonymization, pseudonymization, and encryption of UPD;
	2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems, facilities, and services;
	3. The ability to restore the availability of and access to UPD in a timely manner in the event of a physical or technical incident; and
	4. A process for regularly testing, assessing, and evaluating the effectiveness of technical, physical, and administrative measures for ensuring the security of the Data Processing.
2. The Processor’s measures for protecting UPD shall (a) meet or exceed industry best practices for safeguarding personal data, and (b) be based on the concepts of privacy by design and by default.

# DATA BREACH responsE

1. The Processor shall have sufficient capabilities for detecting, identifying, and responding to a Data Breach.
2. If the Processor has reason to believe that a Data Breach has occurred, then, without undue delay, the Processor shall notify the University of said Data Breach. Such notification to the University shall include sufficient information to enable the University to meet its obligations under applicable law.
3. In the event of a Data Breach, the Processor shall cooperate with the University and immediately:
	1. Investigate and identify the nature of the Data Breach;
	2. Preserve relevant evidence;
	3. Contain, remediate, and mitigate the Data Breach; and
	4. Notify the University of any additional or newly-emerged information beyond the initial Data Breach notification to the University described in § H.2.
4. In the event of a Data Breach caused in whole or part by the Processor:
	1. The University may instruct the Processor, at the Processor’s expense, to provide:
		1. Notice when required by applicable law, or when a Data Breach could result in harm to individuals and/or risk to the University; and/or
		2. Services such as credit monitoring or identity theft protection to individuals when the absence of such services could result in harm to individuals and/or individuals would have a reasonable expectation that such services be provided.
	2. Alternatively, the University may elect to provide the aforementioned notice and services itself.
5. Notwithstanding the foregoing, unless the Processor is required by law to provide the aforementioned notice and/or services in a particular manner, the University shall control the time, place, content, and manner of such notice and services.

# DISPOSITION OF UPD UPON Termination OR FULFILLMENT OF PURPOSE

* 1. The duration of Data Processing by the Processor shall be no longer than the expiration or termination of the Agreement or fulfillment of the Purpose with respect to UPD, whichever is earlier.
	2. Upon expiration or termination of the Agreement, or fulfillment of the Purpose with respect to UPD, whichever is earlier, the Processor shall transfer to the University any and all UPD, unless otherwise instructed by the University in writing.

# gENERAL TERMS

1. SURVIVAL AND ORDER OF PRECEDENCE. This DPA shall survive the expiration or earlier termination of the Agreement. In the event the provisions of this DPA conflict with any provision of the Agreement, or the Processor’s warranties, support agreement, or service level agreement, the provisions of this DPA shall prevail.
2. SEVERABILITY. If any provision of this DPA is found to be unenforceable, the remainder of the Agreement and this DPA shall remain in effect.
3. HEADINGS FOR CONVENIENCE ONLY. Any and all subject headings are not substantive and are for convenience only.
4. NOTICES. Any notices or communications required or permitted to be given by this DPA must be (a) given in writing, and (b) personally delivered; mailed by prepaid, certified mail, or overnight courier; or transmitted by electronic mail (including PDF) with receipt acknowledged, to the party to whom such notice or communication is directed, or to the mailing address or regularly monitored electronic email address of such party.

**IN WITNESS WHEREOF, this DPA has been executed as of the date of the last party to sign below (“Effective Date”). If signed in counterparts, then each shall be considered an original thereof.**

|  |  |
| --- | --- |
| **University:**Signature | **Processor:**Signature |
| Name and Title | Name and Title |
| Date | Date |

**DESCRIPTION OF DATA PROCESSING EXHIBIT**

This Description of Data Processing Exhibit to the Data Processing Agreement (the “DPA”) sets forth certain information relating to the Data Processing, current as of the date of the last signature below (including in a countersigned version of this Description of Data Processing Exhibit), that the Parties anticipate will be carried out in connection with the Work as defined in the DPA. This version of this Description of Data Processing Exhibit may be superseded by subsequent versions issued in accordance with Section § D.2 of the DPA.

1. **NATURE AND PURPOSE**

[Describe the nature (such as the operations to be undertaken by the Processor, volume of personal data, etc.) and the purpose (such as the University’s mission and the University department or unit’s specific objectives that will be fulfilled through the Processor’s Data Processing)]

1. **CATEGORIES OF DATA SUBJECTS**

[List the categories of individuals about whom personal data relates (such as currently enrolled undergraduate students, prospective academic personnel, alumni who have donated to the University between 2008-2018, etc.)]

1. **TYPES OF PERSONAL DATA**

[List the personal data points that will undergo Data Processing including any special categories of personal data. NOTE: special categories of personal data include information relating to 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.]

1. **PROCESSOR CONTACT PERSON**

[Insert name, title, mailing address, email address, and phone number]

1. **UNIVERSITY DEPT/UNIT CONTACT PERSON**

[Insert name, title, mailing address, email address, and phone number]

1. **SUB-PROCESSORS**

[The Processor must list all Sub-processors that will perform any GDPR-governed Data Processing (such as cloud storage providers, hosting providers, etc.), with an explanation of each Sub-processor’s Data Processing activities. If GDPR does not apply or the Processor does not use any Sub-processors for GDPR-governed Data Processing, insert “Not Applicable”.]

|  |  |
| --- | --- |
| **University:**Signature | **Processor:**Signature |
| Name and Title | Name and Title |
| Date | Date |