UW Units should use this decision support tool to help understand and determine the:

* Identifiability of data as Personal Data;
* Applicability and need for a Data Processing Agreement (DPA) and/or Standard Contractual Clauses;
* UW unit’s role in the Data Processing; and
* Third Party’s role in the Data Processing.

For more in-depth information about DPAs, step-by-step workflow processes, and additional self-help resources, see the Privacy Office Data Processing Agreement webpage at <https://privacy.uw.edu/design/agreements/dpa/>.

UW Unit: [insert Name]
Third Party: [insert Name]
Third Party Project, Product, Service, or Activity: [insert name of project, product, service, or activity]

# Determine identifiability and applicability

Definitions in this section are copied from the UW Privacy Office Glossary of Terms at <https://privacy.uw.edu/education/glossary/> and included below for your convenience.

If you answer yes to a question in this section, then proceed to the next question. You need to answer all questions in this section unless instructed to proceed to a different section.

* 1. **Does the project, product, service, or activity involve Personal Data as defined below?**

Personal Data are any record 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. Personal Data includes or may be referred to as personally identifiable data (or a similar term) in UW operational practices or by any applicable law.

Pseudonymized Data is a type of Personal Data. Data are considered pseudonymized if direct identifiers have been eliminated, transformed or replaced by other values, and indirect identifiers may remain intact. Re-identification may occur where there is failure to secure the pseudonymization method or key used, and/or when reverse engineering is successful.

De-identified Data is a type of Personal Data. Data are considered de-identified if direct and known indirect identifiers (perhaps contextually identified by a particular law or regulation, e.g., HIPAA) have been removed or mathematically manipulated to break the linkage to identities. Re-identification may still be possible through a variety of techniques. If re-identification of the data is possible, it is still Personal Data.

Anonymized Data are not Personal Data. Data are considered anonymized if: a) the data and/or information does not relate to an identified or identifiable natural person; or b) the Data Subject is not or is no longer identifiable, even when using additional data.

* + **Yes**
	+ **No** – *A DPA is not required for data that are not Personal Data. Proceed to SECTION 6: ATTESTATION.*
	1. **Are the Personal Data either unencrypted or encrypted and available for the Third Party to decrypt the Personal Data or otherwise process Personal Data in the (i.e., available in an unencrypted form)?**
	+ **Yes**
	+ **No** – *A DPA is not required for encrypted data that cannot be decrypted or processed in an unencrypted form by the Third Party. For example, when Personal Data are stored in an encrypted form in a third-party cloud service and the Third Party cannot decrypt the Personal Data. Proceed to SECTION 6: ATTESTATION.*
	1. **As part of the relationship, does the Third Party perform Data Processing of Personal Data, such as access, adaptation, alteration, analysis, combination of data sets, collection, consultation, disclosure by transmission, dissemination, deletion, organization, retrieval, recording, storage, or use?**

Note: While supporting software that is installed on UW systems or UW’s instances of cloud systems a vendor may view Personal Data, triggering the need for a DPA.

* + **Yes**
	+ **No** – *A DPA is not required if the Third Party is not processing Personal Data. Proceed to SECTION 6: ATTESTATION.*

If you answered Yes to all of the questions in this section, then proceed to the next section.

# Determine the Unit’s need for DPA

* 1. **Does the proposed Third Party processing of Personal Data involve high-risk processing?** Check all that apply. For more information see the UW Privacy Office’s DPA webpage at [https://privacy.uw.edu/design/agreements/dpa/.](https://privacy.uw.edu/design/agreements/dpa/)
* **Yes,** automated decision-making with legal or similar significant effect (i.e., no human involvement or intervention in the decision-making)
* **Yes,** data concerning vulnerable Data Subjects (e.g., children, elderly, those with certain health conditions, etc.)
* **Yes,** data processed on a large scale
* **Yes,** datasets that have been matched or combined
* **Yes,** evaluation or scoring
* **Yes,** innovative use or new technology
* **Yes,** interference with rights or opportunities
* **Yes,** sensitive data or data of a highly personal nature
* **Yes,** systematic monitoring
* **Yes,** other high risks to the fundamental rights or freedoms of individuals
* **Yes,** other high risks (such as targeted advertising, sale of Personal Data (i.e., trade for value))
* **No,** the processing of Personal Data does not involve any of the above high-risk processing

*Note: If the Data Processing involves high-risk processing, then a Privacy Impact Assessment must be completed before engaging with and/or signing an agreement with a Third Party that is processing Personal Data.*

* 1. **Are there laws or regulations (e.g., FERPA, GLBA, etc.) that impart a duty to the UW to protect the Personal Data that are involved in the proposed Third Party processing?** For more information see UW Privacy Office’s webpage on laws and regulations at <https://privacy.uw.edu/policies/laws/>?
	+ **Yes**
	+ **No**
	+ **Unknown**
	1. **Does the proposed Third Party processing of Personal Data involve data that are associated with students’ affiliation at the UW (e.g., student username, password, email address, grades, demographic data etc.)?**
	+ **Yes**
	+ **No**
	1. **Does the proposed Third Party processing of Personal Data involve username or email address, in combination with a password or security questions and answers that would permit access to an online account, for more than twenty employees within your UW unit who will use the service for benchmarking, reference material, or optional training?** For example, access to Gartner insights or other reference material.
	+ **Yes**
	+ **No**

If you answered yes to one or more of the questions in this section, then proceed to the next section. If you answered no or not applicable to all the questions in this section, then you do not need a DPA. Proceed to SECTION 6: ATTESTATION.

# Determine type of THIRD-PARTY relationship and applicable agreement

* 1. **What is the UW Unit’s role in Data Processing?**
	+ [**Controller**](https://privacy.uw.edu/education/glossary/) (aka Data Controller—the person or entity that determines the purpose and means for Data Processing)
	+ [**Processor**](https://privacy.uw.edu/education/glossary/)(aka Data Processor—the person or entity that performs Data Processing on behalf of the Controller)
	+ **Both** (e.g., when UW processes Personal Data in Workday)
	1. **What is the Third Party’s proposed role in Data Processing?**
	+ **Controller**
	+ **Processor**
	+ **Both**

If UW is the Controller and the Third Party is the Processor, then a UW Controller-to-Processor DPA (or agreement with equivalent privacy and data protection terms and conditions) is required. Proceed to SECTION 5.

If UW is both a Controller and a Processor and the Third Party is the Processor, then a UW Controller-to-Processor DPA (or agreement with equivalent privacy and data protection terms and conditions) is required. Proceed to SECTION 5.

If UW is the Controller and the Third Party proposed that they are also a Controller, then you need to determine if the Controller-to-Controller relationship is appropriate for the UW and its constituents. Proceed to SECTION 4.

If UW is a Processor and the Third Party is the Controller or both a Controller and Processor, then a DPA is not required by UW but may be required by the Third Party. Proceed to SECTION 6.

# Establish appropriate boundaries on Controller-to-Controller relationship

* 1. **Does the proposed agreement include appropriate limits on the use of the State of Washington resources (e.g., UW data, network, systems, facilities, and/or University personnel) for private gain?** See RCW 42.52.160 at <https://apps.leg.wa.gov/rcw/default.aspx?cite=42.52.160>. State resources may include, but are not limited to UW data, network, systems, facilities, and/or University personnel.
	+ **Yes**
	+ **No**
	+ **Unknown**
	1. **Is the proposed Third Party processing of Personal Data allowed under UW Administrative Policy Statements (APS), Executive Orders (EO) or other rules?** See UW Policy and Rules at https://www.washington.edu/admin/rules/policies/#gsc.tab=0.
	+ **Yes**
	+ **No**
	+ **Unknown**
	+ **Not applicable since Third Party is not a Data Controller**
	1. **Does the proposed Third Party processing** **of Personal Data exclude high-risk processing?** Check all that apply.
	+ **Yes,** excludes automated decision-making with legal or similar significant effect (i.e., no human involvement or intervention in the decision-making)
	+ **Yes,** excludes data concerning vulnerable Data Subjects (e.g., children, elderly, those with certain health conditions, etc.)
	+ **Yes,** excludes data processed on a large scale
	+ **Yes,** excludes datasets that have been matched or combined
	+ **Yes,** excludes evaluation or scoring
	+ **Yes,** excludes innovative use or new technology
	+ **Yes,** excludes interference with rights or opportunities
	+ **Yes,** excludes sensitive data or data of a highly personal nature
	+ **Yes,** excludes systematic monitoring
	+ **Yes,** excludes other high risks to the fundamental rights or freedoms of individuals
	+ **Yes,** excludes other high risks (such as targeted advertising, sale of Personal Data (i.e., trade for value))
	+ **No,** the processing of Personal Data does not involve any of the above high-risk processing
	1. **Are Data Subjects informed about and given a choice whether to participate in processing of Personal Data for the Third Party’s purpose that is supplemental to the UW’s purpose for Data Processing without foregoing the intended benefit or value from the UW’s purpose for Data Processing?**
	+ **Yes,** Data Subjects can opt-in to processing for the Third Party’s purpose(s) that is supplemental to the UW’s purpose
	+ **Yes,** Data Subjects can opt-out of processing for the Third Party’s purpose(s) that is supplemental to the UW’s purpose
	+ **No,** Data Subjects are not given a choice about the processing Personal Data for the Third Party’s purpose that is supplemental to the UW’s purpose
	1. **Does the Third Party’s purpose that is supplemental to the UW’s purpose benefit or provide opportunity to the Data Subjects in a way that the Data Subjects would not otherwise be able to obtain (e.g., continuity of essential healthcare services, access to library resources that are for academic purposes and cost prohibitive for the Data Subjects)?**
	+ **Yes**
	+ **No**
	+ **Unknown**

If the UW is the Data Controller and the Third Party proposed that they are also a Data Controller in SECTION 3 above, and you answered “yes” to all applicable questions in SECTION 4, then the UW Controller-to-Controller DPA (or agreement with equivalent privacy and data protection terms and conditions) is seemingly appropriate and required.

If you answered “no” or “unknown” to any of the questions in SECTION 4, then send a copy of your completed decision support tool to the UW Privacy Office at uwprivacy@uw.edu and request additional guidance for establishing appropriate boundaries for the proposed Controller-to-Controller relationship.

# Determine need for standard contractual clauses

In addition to a DPA, in some situations involving data transfers across country lines, Standard Contractual Clauses may be needed. Note that this can include using cloud servers based in foreign countries. Standard Contractual Clauses are related to the European Union-approved set of contract terms that will be appended to the agreement or contract when data are transferred from the European Economic Area.

* 1. **Does the proposed processing of Personal Data involve the transfer of Personal Data from any country that is a member of the European Economic Area (EEA)?** See list of EEA members is available at <https://www.eea.europa.eu/countries-and-regions> to a country or countries outside the EEA.
	+ **Yes**
	+ **No**
	1. **Does the proposed processing of the Personal Data involve the transfer of Personal Data from the EEA without the direct participation of the Data Subjects?**

Note: Direct participation of the Data Subjects includes, for example, Data Subjects inputting their own data into a web form.

* + **Yes**
	+ **No**
	1. **Do the destination countries lack laws with adequate protections to the GDPR as determined by the European Council?**

Note: Adequacy decisions are listed by the European Commission at <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. As of May 1, 2022, most nations, including the United States, do not have adequacy decisions.

* + **Yes**
	+ **No**

If you answered yes to all the questions in this section, then the Standard Contractual Clauses are required in addition to any necessary DPA. Along with other restrictions, the SCCs have specific requirements for Onward Transfers. For more information see the Privacy Office DPA webpage at <https://privacy.uw.edu/design/agreements/dpa>.

# Attestation

I have read and understand the information provided on the Privacy Office’s website about DPAs and Standard Contractual Clauses. I confirm the above is true to the best of my knowledge. I confirm I am the person in the UW Unit who is responsible for managing the above third-party relationship and updating the agreement if the above circumstances change.

First and Last Name: [insert full name]
Signature:
Job Title: [insert job title]
Date: [insert date]