Office of Legal Affairs
UNIVERSITY OF WISCONSIN–MADISON

European Union (EU) General Data Protection Regulation (GDPR)
UW-Madison Guidance for Contracting and Research

GDPR is a European law that establishes data protections for privacy and security of **personal data** about individuals in the European Economic Area (EEA) that includes the 28 countries in the European Union (EU) and Norway, Iceland, and Lichtenstein. GDPR applies to U.S.-based universities acting as a controller or a processor in processing the personal data of data subjects located in the European Economic Area (EEA). This document outlines guidance for addressing GDPR issues in contracts and regarding research conducted by the university. It includes a step-by-step process for analyzing whether GDPR applies, and directions to follow when it does. Applicable definitions of relevant terms are the definition section of this document. **These terms have specific meaning under GDPR and need to be reviewed and understood to appropriately process contracts and conduct research.**

I. What does GDPR cover?

Unlike data privacy and security laws in the U.S., which tend to be directed to specific types of data (e.g., health information, student information), GDPR applies to the collection and use of all personal information:

- Through activities within the borders of EEA countries
- That is related to offering goods or services to subjects within the EEA, or
- That involves monitoring the behavior of subjects within the EEA.

II. What Countries are subject to GDPR?

The EEA countries that have adopted GDPR are Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom.

III. Why does this matter to UW-Madison?

Where the university is working with personal data collected in, or transferred from, any of the above countries, GDPR will be relevant. Failure to follow GDPR's regulations if they apply puts the University at risk of noncompliance, monetary fines, and reputational harm. Fines associated with noncompliance under the GDPR can be up to 20 million Euros or 4% of the University's prior financial year worldwide annual revenue.

IV. How does this apply to Contracts?

A. Introduction

GDPR protects personal data of individuals who are located in the EEA and referred to as "data subjects." Under GDPR, UW-Madison can be a controller or a processor. Controllers bear most of the responsibility for compliance with GDPR. Processors have some regulatory requirements but mostly are subject to requirements through contractual provisions that Controllers must enforce with Processors. Below is a process for analyzing whether GDPR applies and, if so, what are the appropriate contract provisions. **Review of the defined terms at the end of this document is critical for answering the below questions.**

B. Contract Review Process

As noted above, GDPR applies to organizations located in the EEA and to organizations located outside of the EEA if they offer goods or services to, or monitor the behavior of EEA data subjects. It also applies to all organizations processing or holding the personal data of data subjects residing in the EEA, regardless of the organization's location. UW-Madison will likely be subject to GDPR under the second prong (offering goods and services to or monitoring the behavior of EEA data subjects) or where we are processing or holding EEA data subjects' personal data. Contracts involving GDPR will focus on data processing, so start by asking whether the contract involves processing personal data of data subjects residing in the EEA.

1. Does the contract involve processing personal data of data subjects in the EEA? If no, then GDPR likely does not apply and no DPA is required.
    a. If the data to be processed is anonymized (i.e., not merely pseudonymized), it is not subject to GDPR.
    b. If the data to be processed does not relate to individuals located in the EEA and we are processing it with a non-EEA entity, it will generally not be subject to GDPR and not require a DPA. However, if we transfer data to an entity in the EEA for processing, that entity will require a DPA because it is required under GDPR to protect all personal data it receives, regardless of the data subject's nationality or residence.
2. If the answer to 1 is yes, a DPA is required and the university needs to ensure that there is a recognized and documented lawful basis under GDPR for processing the data. Request this information from the university unit seeking the contract and consult with Office of Legal Affairs to review the purported lawful basis.
3. Next, determine whether the personal data to be processed contains any special categories of personal data that will merit a higher level of protection. If no special category personal data is present, we only need to establish the general lawful basis for the processing. If a special category is present we need to ensure that there is a recognized and documented lawful basis for the processing the data AND identify a special category condition from the list in Article 9(2) of the GDPR.
4. The next question is whether the University is the controller or the processor. If we are the controller, we need to ensure that appropriate provisions as described below

are in a DPA. Often a processor that is subject to GDPR will present us with a DPA because it knows that one will be required for them to perform the necessary processing activities. If we are the processor, the controller will present us with a DPA instructing us how to process the personal data in its possession. Below are the required provisions in any DPA involving GDPR-covered personal data. A sample agreement with options is also included in this document.

Controllers:

a. May only use processors that provide sufficient guarantees that appropriate technical and organizational measures exist to ensure the processing will meet GDPR requirements and protect data subject rights

b. Must have and identify an appropriate lawful basis under GDPR (Article 6) for processing the data.

c. Must establish written contract (DPA) with processor that documents and includes clauses that address the following:

    i. Subject matter and duration of the processing

    ii. Nature and purpose of the processing

    iii. Type of personal data and categories of data subjects

    iv. Obligations and rights of the Controller

    v. Specific requirements for processors

    vi. Only processing personal data per instructions of the Controller

    vii. Individuals authorized to process the personal data commit to confidentiality or are under appropriate statutory obligation of confidentiality

    viii. Implementation of appropriate technical and organizational measures to ensure security of data including, as appropriate: pseudonymization; encryption; ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services; ability to restore availability and access to personal data in timely manner, and process for testing, assessing and evaluating effectiveness of the measures to ensure security of processing

    ix. Obtaining prior specific or general written authorization from Controller to engage a sub-contractor and pass contractual obligations on the processor to the sub-contractor to meet as well

    x. Assisting the Controller with the following:

        a. Responding to requests related to Data Subject's Rights

b. Implementing appropriate technical and organizational measures to ensure level of security appropriate to the risk

c. Notification of personal breach to Supervisory Authority and to data subject – processor must notify controller without undue delay once it becomes aware of a personal data breach and assist with providing information relevant to providing notification

d. Performing Data Protection Impact Assessment where appropriate

xi. Deleting or returning Controller data based on Controller's preference

xii. Cooperating with Audit Rights of Controller

5. The last question - do the processing activities under the agreement involve an International Data Transfer, also known as a restricted transfer? GDPR restricts transfers of personal data outside the EEA, or the protection of the GDPR, unless the personal data is protected in another way, or one of a limited number of exceptions applies. Here is the process for assessing restricted transfers:

   a. Does the contract involve making a restricted transfer of personal data outside of the EEA? If no, the transfer can occur. If yes, go to the next question.

   b. Do we need to make a restricted transfer of personal data in order to meet our purposes? If no, make the transfer without sending any personal data. If yes, go to the next question.

   c. Has the EU made an 'adequacy decision' in relation to the country or territory where the receiver is located or a sector which covers the receiver? If yes, you can make the transfer. If no, go to the next question. Note that the U.S. is not fully approved as a jurisdiction with adequate data protection legislation. Only companies that register with the Privacy Shield are deemed "adequate." Non-profits like universities are ineligible to register for the Privacy Shield.

   d. Have we put in place one of the 'appropriate safeguards' referred to in the GDPR? If yes, you may go ahead with the restricted transfer. If no, go to the next question. Here are the appropriate safeguards:

      i. **A legally binding and enforceable instrument between public authorities or bodies.** A public authority or body can make restricted transfers to another public authority or body where both have signed a contract that includes enforceable rights and effective remedies for individuals whose personal data is transferred. It is undecided under GDPR whether public universities like UW-Madison are public authorities or

bodies. We don't recommend relying on this safeguard without additional guidance from the EU.

ii. **Binding corporate rules.** Allows a restricted transfer if both the sender and the receiver have signed up to a group document called binding corporate rules (BCRs). UW-Madison does not qualify for this safeguard. BCRs are an internal code of conduct operating within a multinational group, which applies to restricted transfers of personal data from the group's EEA entities to non-EEA group entities. This may be a corporate group or a group of undertakings or enterprises engaged in a joint economic activity, such as franchises or joint ventures. BCRs must be submitted for approval to an EEA supervisory authority in an EEA country where one of the companies is based.

iii. **Standard data protection clauses adopted by the Information Commissioner's Office (Commission).** These are known as the "standard contractual clauses" (sometimes as "model clauses") that must be entered into by the data exporter (based in the EEA) and the data importer (outside the EEA). {(See sample DPA with optional clauses including standard contractual clauses) The clauses contain contractual obligations on the data exporter and the data importer, and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and the data exporter. There are problematic clauses for the University as a state entity related to liability, mediation, jurisdiction, and governing law. However, the standard contractual clauses must be used **in their entirety and without amendment**. Even if a project does not involve a restricted transfer, the standard DPAs often include provisions that account for the possibility of such a transfer by noting that if such a transfer is part of the processing, then the processor and controller agree to comply with the standard contractual clauses. Clauses on business related issues may be added provided that they do not contradict the standard contractual clauses. Parties (i.e. additional data importers or exporters) can be added provided they are also bound by the standard contractual clauses.

iv. **An approved code of conduct together with binding and enforceable commitments of the receiver outside the EEA.** If the receiver has signed a code of conduct that is approved by a supervisory authority, the transfer can be made. The code of conduct must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced. While GDPR endorses approved codes of conduct, there are no approved codes in use yet.

v. **Certification under an approved certification mechanism together with binding and enforceable commitments of the receiver outside the EEA.** Transfer can be made if the receiver has a certification under a scheme approved by a supervisory authority. The certification scheme must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced. While GDPR endorses their use, no approced certification schemes are in use yet.

vi. **Contractual clauses specifically approved by a supervisory authority.** These are not in use yet, pending additional guidance.

e. Does an exception provided for in the GDPR apply? If yes, transfer can be made. If no, the transfer may not be made. If you reach the end without finding a provision which permits the restricted transfer, you will be unable to make that restricted transfer in accordance with the GDPR. Here are the exceptions or derogations (generally, consent or performance of contract will be the appropriate basis since U.S.-based universities will have a difficult time meeting the other derogations):

a. Specific consent from individual whose data is to be transferred. Must tell them the identity of the receiver, or the categories of receiver; the country or countries to which the data is to be transferred; the need for the restricted transfer; the type of data; the individual's right to withdraw consent; and the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place. Consent must be capable of being withdrawn which means it may not always be the best solution.

b. Transfer needed for performance of contract to which data subject is a party. This exception works for occasional restricted transfers. If making regular transfers, need to adopt an appropriate safeguard.

c. Transfer necessary for important reasons of public interest. Requires an EU or Member state law that states or implies this type of transfer is allowed for important reasons of public interest. Also not suitable for regular transfers.

d. Transfer necessary to determine if you have a legal claim, to make a legal claim, or to defend a legal claims.

e. Transfer necessary to protect the life of an individual. May not use this exception to carry out general medical research. Only applies where the person is physically and legally *incapable* of giving consent.

f. A one-off transfer made in organization's legitimate interests. Very restricted and only to be used where none of the safeguards or exceptions apply. Transfer can't be repetitive and must relate to only a limited number of individuals. The supervisory authority and the individual whose data will be transferred must be informed about the transfer.

C. Contract Review - Implementation Procedures

1. It is critical that the reviewer of any contract subject to GDPR obtain answers to the following key questions to ensure a proper review for GDPR compliance.

a. What is the personal data to be processed and does it include any of the special categories of personal data that are subject to additional restrictions/requirements?

b. What is the GDPR-approved lawful basis (Article 6 basis) for processing the personal data? If special categories of personal data are involved, what is the additional Article 9 condition for processing the special categories of personal data?

c. Is a restricted transfer (international data transfer) involved and, if so, are there the appropriate safeguards in place or does an exception apply authorizing the transfer?

D. Contract Review Assistance

As noted above, where the university is the controller, it is imperative that the university's purported lawful basis for the processing be reviewed to determine if it meets the GDPR lawful basis requirements. While the UW-Madison GDPR Implementation Committee determines a final and formal review process, questions and reviews of proposed lawful bases should be directed to the Office of Legal Affairs.

V. RESEARCH

A. How does the GDPR relate to research in general?

1. It establishes the circumstances under which it is lawful to collect, use, disclose, destroy, or otherwise process "personal data."

2. It establishes certain rights of individuals in the EEA, including rights to access, amendment, and erasure (right to be forgotten).

3. It requires researchers to implement appropriate technical and organizational security measures to ensure a level of data security that is appropriate to the risk of the data.

4. It requires notification to data protection authorities and affected individuals within 72 hours following the discovery of a personal data breach, which is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

B. What is Identifiable Personal Data Under GDPR

"Personal data" is any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

"Special categories" of personal data require a higher level of protection due to their sensitive nature and consequent risk for greater privacy harm. This includes information about a data subject's health, genetics, race or ethnic origin, biometrics for identification purposes, sex life or sexual orientation, political opinions, religious or philosophical beliefs, or trade union membership. Although criminal convictions and records are not considered "special categories" of personal data, this information is subject to amplified protections under the GDPR.

Anonymized Data: The GDPR does not apply to data that have been anonymized. However, under GDPR, there is no de-identified (or "anonymized") safe harbor akin to HIPAA. Whether data can be considered anonymized, and therefore not subject to GDPR, must be determined based on the facts and circumstances, considering all the means reasonably likely to be used, either by the person in control of the data ("controller") or by another person, to identify the natural person, directly or indirectly.

Coded or Pseudonymized Data: Data that has been "pseudonymized" (coded data - can no longer be attributed to a specific data subject without the use of key-code information that is kept separately) remains personal data that **IS** subject to GDPR.

C. How Research Activities May Invoke GDPR

First, note that citizenship is irrelevant to whether GDPR applies. For example, EEA citizens who reside in the U.S. would generally not be covered by GDPR, while citizens of other non-EEA countries residing in the EEA generally would be covered.

There are several ways that research activities may invoke GDPR:

a) Activities within the borders of EEA countries, such as conducting a multi-site trial in an EEA member state.

b) Offering goods and services, regardless of whether connected to payment, to data subjects in EEA countries. Examples of arrangements that could be said to offer services to EEA data subjects include providing a mobile application to EEA residents for tracking medication compliance and which transfers such data to the study team, or collaboration agreements with research institutions in EEA countries to share data with U.S. researchers for analysis. Mere accessibility of a website by EEA residents alone is not enough to demonstrate offering a service, but websites aimed at EEA residents could be (e.g., websites aimed at recruiting EEA data subjects into a study).
c) Monitoring behavior of subjects within the EEA, such as reviewing data collection and adverse events related to data subjects in the EEA; collecting information related to EEA data subjects' online presence such as through social media; collecting information about EEA data subjects via online surveys; or tracking their internet browsing.

D. How GDPR Affects Research

GDPR requires a legal basis to collect and process (e.g., analyze) personal data. In order to use personal data for research, the legal basis that *generally* will apply is consent from the data subject.

Consent must be **freely given**, **specific**, **informed** and **unambiguous** as to the data subject's wishes by a **statement** or by a clear **affirmative action**:

a) Freely given means the individual must have a realistic choice, or the realistic ability to refuse or withdraw consent. Individuals in a position of authority cannot obtain consent, nor can consent be coerced.
b) Specific means the consent must be explicit and transparent and contain the following information:
    i. Identity of the Principal Investigator
    ii. Purpose of the data collection
    iii. Types of data collected, including listing of any special categories of data
    iv. The right to withdraw from the research and the mechanism for withdrawal
    v. Identify who will have access to the data
    vi. Time period for which data will be stored (can be indefinite)
    vii. Information regarding data security, including storage and transfer of data
    viii. Information regarding automated processing of data for decision making about the individual, including profiling
    ix. Information regarding data security, including storage and transfer of data
    x. Whether and under what conditions data may be used for future research, either related or unrelated to the purpose of the current study.
c) Informed means that subjects are made aware of the risks, how their data will be safeguarded, their rights in relation to the research (as described below), and how to exercise those rights.
d) Unambiguous means consent is given through a statement or clear affirmative action.

i. This may be by a written or oral statement or other affirmative act demonstrating consent. For instance, checking a box can indicate consent, while silence or pre-ticked boxes that require unchecking (opting out) cannot.
ii. Investigators should be able to demonstrate that a particular subject consented to the research. Consent records, including time and date of consent, must be maintained for each data subject.
iii. If the consent form serves multiple purposes, the request for consent must be clearly distinguishable within the document.
iv. There is no ability for the IRB to waive informed consent under GDPR.

Additionally, there are certain rights that data subjects have:

a) The right of access to their data.
b) The right to request corrections to their data.
c) The right to withdraw and to request erasure of their data. In this case, data may be retained only if it is anonymized or if another legal basis exists to retain the data. This may include:
    i. The need to protect scientific research if deletion would render impossible or seriously impair the research objectives; or
    ii. The need to protect the public health by ensuring the accuracy and quality of data related to medical care or to investigational drugs and devices.
d) The right to request transfer of their personal information to a third party (such as a personal physician) in a format suitable for re-use.

E. Research That May Unintentionally Invoke GDPR

Certain types of research activities are more likely to collect personal data from EEA data subjects without the knowledge or intent of the research team. For instance, data collection from social media platforms could easily contain personal data from EEA data subjects. Similarly, online survey research may enroll EEA data subjects.

Researchers may want to verify where data is coming from by, for example, including a screening question asking whether potential subjects reside in an EEA country. In this case, researchers can ensure the consent form complies with GDRP or can remove a potential subject from the pool.

F. Data Breach – Responsibilities

The GDPR has very strict rules and timelines regarding report of data breaches. Any data breach occurring on a project involving GDPR-covered research must be reported within 24 hours upon identification of the breach to the Office of Legal Affairs (608-263-7400), in addition to any report that must be made to the IRB. The following information should be communicated:

1. Type of breach
2. Nature, sensitivity, and volume of personal data
3. Severity of consequences for individuals

4. Number and characteristics of affected individuals
5. Ease of identification of individuals
6. Protocol number

GDPR Terms – Definitions and Interpretations

1. **Anonymous information**: information which does not relate to an identified or identifiable natural person or personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Anonymous information is **NOT** subject to GDPR.
2. **Consent**: consent of a data subject is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them. Consent can be given via oral or written statement (including an electronic statement such as checking a box when visiting a website) but silence or pre-checked boxes or inactivity are not sufficient. Parental consent is required for processing a minor's personal data. More explicit consent is required for processing certain categories of sensitive data. Consent has to be as easy to withdraw as it was to give. It is not freely given if the data subject is unable to refuse or withdraw consent without detriment.
3. **Controller**: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
4. **Data Subject**: the identifiable natural person located in the EEA whose data is being processed.
5. **European Union**: includes Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. The United Kingdom is expected to continue to be a member of the EEA into 2019.
6. **European Economic Area (EEA)**: includes Iceland, Liechtenstein and Norway and the countries of the European Union. Switzerland is not a member of the EU or the EEA.
7. **International Data Transfer/Cross-Border Processing**: data subject personal data that is held in EU or EEA is transferred to an entity in a jurisdiction outside of the EU or EEA.
8. **Lawful Basis**: To process personal data, we must have one of the six valid lawful bases below. As a U.S.-based entity, we are most likely to rely on consent, contract, and legitimate interests. Legal obligation refers only to legal requirements under EU or member state law, and the public task is related to EU or member state established public interest/official functions/law.
    a. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
    b. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
    c. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d. Vital interests: the processing is necessary to protect someone's life.

e. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

9. **Minor**: EU defines as children under the age of 16, but member states may lower the age to as low as 13. Processing minor personal data requires consent of authorized holder of parental responsibility over the child. The controller is required to use "reasonable efforts" to verify validity of the consent. Reasonable efforts are not defined.

10. **Monitoring of Behavior as it occurs in EEA**: Data subject being tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling an individual to make decisions regarding them or for analyzing or predicting their personal preferences, behaviors, and attitudes. Profiling is the automated analysis or predicting of behavior, location, movements, reliability, interests, personal preferences, health, economic situation, performance, etc. Monitoring and profiling include online monitoring and behavioral-based advertising that creates profiles bases on the data subject's actions, travel data of individuals using city's public transport system (e.g., tracking via travel cards), profiling and scoring for purposes of risk assessment (e.g., credit scoring, establishing insurance premiums, fraud prevention, detection of money laundering), location tracking (e.g., mobile apps), monitoring of wellness, fitness and health data via wearable devices. May also include CCTV, smart cars, home automation, and how employers collect information on their employees inside and outside of the work place.

11. **Offering Goods and Services to Data Subjects**: Where it is apparent that the controller or processor intends to offer services to data subjects in one or more EEA member states. Mere accessibility of controller's or processor's website, email address or other contact details, or use of language generally used in the country where controller is established is insufficient to equal such intent. Factors that may demonstrate such intent include international telephone numbers on their website for contact purposes, using top level domains of an EU Member State (i.e. .eu, .ie, .de), providing options for EEA language translation, providing options for EU currency conversion, and advertising to attract EEA users (leveraging existing EEA clients or users as advertising material).

12. **Personal Data**: any information relating to an identified or identifiable natural person. Identifiable natural person is one who can be identified directly or indirectly by reference to an identifier such as a name, identification number, location data, online identifier, or factor specific to physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples include name, photo, email address, bank details, posts on social media, medical information, IP addresses, mobile device identifiers, biometric data, and geolocation tags. **GDPR does not apply to deceased persons.**

13. **Processing**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. If UW-Madison processes data from such data subjects for itself or for another entity, GDPR applies and needs to be addressed. Processing includes 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.

14. **Processor**: any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

15. **Pseudonymization**: processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organization measures to ensure that the personal data are not attributed to an identified or identifiable person. Pseudonymized data **IS** subject to GDPR.

16. **Special Categories of Personal Data**: referred to as sensitive data and includes race, ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetics, biometric data where used for identification purposes, health, sex life, or sexual orientation. Processing these categories of data is prohibited unless we identify a lawful basis under Article 6 of the GDPR (see definition above) AND also identify a special category condition from the list in Article 9(2) of the GDPR which below:

    a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where EU or Member State law provide that the prohibition may not be lifted by the data subject;

    b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

    c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (i.e., processing personal data to save or protect someone's life);

    d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are manifestly made public by the data subject;

f. processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the appropriate conditions and safeguards;

i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

VI. Data Processing Agreement (DPA) – Template

Data Processing Agreement - Template

This Data Processing Agreement ("DPA") dated *month day*, *year* ("Addendum Effective Date') forms part of the Master Service Agreement ("MSA") between: *Company*, d'b/a *Company* ("*Company*"); and the Board of Regents for the University of Wisconsin System on behalf of the University of Wisconsin-Madison (Client or University).

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the MSA. Except as modified below, the terms of the MSA shall remain in full force and effect.

The parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the MSA.

1. Definitions.
   1.1. "Client Personal Data" means any Personal Data Processed by XXXXXX or any XXXXXX Affiliate on behalf of Client or any Client Affiliate pursuant to or in connection the MSA or any related Statement of Work (SOW);

   1.2. "Affiliate" means an entity that is owned or controlled by or is or under common control or ownership with either Client or XXXXXX respectively, 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 securities, by contract or otherwise;

   1.3. "Controller", "Processor", "Data Subject", "Personal Data", "Processing", "Supervisory Authority", "Personal Data Breach" and "Special Categories of Personal Data" shall have the same meaning as in the Data Protection Laws;

   1.4. "Data Protection Laws" shall mean Directive 95/46/EC and Directive 2002/58/EC, in each case as transposed into domestic legislation of each Member State of the European Economic Area and in each case as amended, replaced or superseded from time to time, including without limitation by the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR") and any data protection laws substantially amending, replacing, or superseding the GDPR following any exit by the United Kingdom from the European Union, or, and to the extent applicable, the data protection or privacy laws of any other Member State of the European Economic Area;

   1.5. "EEA" means the European Economic Area as well as any country for which the European Commission has published an adequacy decision as published at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu

   1.6. "Restricted Transfer" means the onward transfer of Client Personal Data that is located in the EEA to XXXXXX in a country that is not in the EEA, where such transfer would be

Commented [LN1]: Represents Template for when the University is a controller and is contracting with a processor to process personal data covered by GDPR. Similar terms will be presented to the University when it serves as a processor for GDPR-covered personal data.

Commented [LN2]: Definitions can be adjusted as necessary depending on the subject matter of the agreement and the need to provide for additional defined terms. These represent a sampling of standard defined terms.

prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses or another adequate transfer mechanism as approved by the European Commission;

1.7. "Standard Contractual Clauses" or sometimes also referred to the "EU Model Clauses"; and

1.8. "Subprocessor" means any Processor (including any third party and any XXXXXX Affiliate) appointed by XXXXXX to Process Client Personal Data on behalf of Client or any Client Affiliate.

2. Subject Matter and Duration. While providing the Services to Client and Client Affiliates pursuant to the MSA, XXXXXX and XXXXXX Affiliates may Process Client Personal Data on behalf of Client or any Client Affiliate as per the terms of this DPA. XXXXXX agrees to comply with the following provisions with respect to any Client Personal Data submitted by or for Client or any Client Affiliate to the Services or otherwise collected and processed by or for Client or any Client Affiliate by XXXXXX or any XXXXXX Affiliate.
   2.1. Subject Matter. The subject matter of this DPA results from the MSA. Under the MSA, XXXXX agrees to [Insert terms] _____
   2.2. Duration. This DPA will end on completion of by XXXXX of the data processing activities described in the MSA and herein.

3. Specification
   3.1. Nature and Purpose of the processing. XXXXX will process XXXX.
   3.2. Geographic Scope. [If needed, insert any geographical limitations for where the processing must occur and how processing results can be retrieved or accessed. This is where it is identified whether there is a restricted transfer of personal data outside of the EEA and a description of the basis justifying the restricted transfer]
   3.3. Type of Data. The subject matter of the processing is XXXXX.
   3.4. Categories of Data Subjects. Data subjects are XXXXX.

4. Controller Obligations and Rights. Client shall be responsible for: (a) giving adequate notice and making all appropriate disclosures to Data Subjects regarding Client's use and disclosure and XXXXXX's processing of Client Personal Data; and (b) obtaining all necessary rights, and where applicable, all appropriate and valid consents to disclose such Client Personal Data to XXXXXX and to permit the processing of such Client Personal Data by XXXXXX for the purposes of performing XXXXXX obligations under the Agreement or as may be required by Data Protection Laws. Client shall notify XXXXXX of any changes in, or revocation of, the permission to use, disclose, or otherwise process Client Personal Data to the extent that such changes may affect XXXXXX's use, disclosure, or other processing of Client Personal Data or otherwise affect XXXXXX's ability to comply with the MSA, or applicable Data Protection Laws. XXXXXX shall not Process Client Personal Data other than on Client's documented instructions unless Processing is required by Data Protection Laws to which XXXXXX is subject, in which case XXXXXX shall to the extent permitted by Data Protection inform Client of that legal requirement before Processing Client Personal Data For the avoidance of doubt, the Agreement and any related SOW entered into by Client shall be constitute documented Instructions for the purposes of this DPA.

Commented [LN3]: Sample language - Company will process sample analysis results received from Client which may contain personal data for quality control purposes and to forward electronic means of access to final results to Client. These processing activities are carried out by Company in performance of its obligations to Client under the MSA.

Commented [LN4]: Sample language - The contractually agreed processing of personal data for quality control purposes by ____ shall be carried out within a member state of the European Union (EU). Access to final results will be provided to Client to access electronically from Wisconsin, USA. This constitutes transfer of personal data outside the EU and an adequate level of protection is provided for this transfer through the Standard Data Protection Clauses, **Appendix 2** (Article 46 Paragraph 2 Points c and d GDPR);

Commented [LN5]: Sample language for 3.3 and 3.4 – The subject matter of the processing is research data. Data subjects are participants in ____ .

5. Confidentiality. XXXXXX shall take reasonable steps to ensure that individuals that process Client Personal Data are subject to obligations of confidentiality or are under an appropriate statutory obligation of confidentiality.

6. Technical and Organizational Measures.
   6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, XXXXXX shall in relation to Client Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
   6.2. XXXX undertakes to give Client the necessary information on request and, in particular to demonstrate the execution of the Technical and Organizational Measures. Evidence of such measures may be provided by:
      6.2.1. Compliance with approved Codes of Conduct pursuant to Article 40 GDPR; and/or
      6.2.2. Certification according to an approved certification procedure in accordance with Article 42 GDPR; and/or
      6.2.3. Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor); and/or
      6.2.4. A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

7. Subprocessing.

   7.1. XXXXX may commission subcontractors (additional contract processors) only after prior explicit written or documented consent. Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Subcontractor	Address/country	Service

   7.2. If the subcontractor provides the agreed service outside the EU/EEA, XXXX shall ensure compliance with EU Data Protection Regulations by appropriate measures.

   7.3. Further outsourcing by the subcontractor is not permitted.

8. Data Subject Rights. XXXXXX shall promptly notify Client if it receives a request from a Data Subject under any Data Protection Laws respect to Client Personal Data. In the event that any Data Subject exercises any of its rights under the Data Protection Laws in relation to Client Personal Data, XXXXXX shall use reasonable commercial efforts to assist Client in fulfilling its obligations as Controller following written request from Client. XXXX may not on its own authority address a Data Subject's exercise of its rights, but only on directions from Client.

Commented [LN6]: Optional – may add two paragraphs that address the technical and organizational measures to be taken and a statement that they are accepted by the controller. Sample language:
1) The necessary technical and organizational measures are documented in Appendix 1 and are hereby approved by the University. The documented measures form the foundation of this DPA. Any amendments shall be implemented by mutual agreement.
2) The technical and organizational measures are subject to technical progress and further development. XXXX may implement alternative adequate measures so long as the security level of the defined measures is not reduced. Substantial changes must be agreed upon by the parties and documented in Appendix 1.

Any Appendix would cover the specifics of the principal technical and organizational measures: confidentiality, integrity, availability and resilience of processing systems and services; ability to restore availability and access to personal data in timely manner, and procedures for testing, assessing and evaluating effectiveness of the measures to ensure security of processing.

Commented [LN7]: Another Option for language: XXXXXX may engage such Subprocessors as XXXXXX considers reasonably appropriate for the processing of Client Personal Data in accordance with this DPA provided that XXXXXX shall notify Client of the addition or replacement of such Subprocessor and Client may, on reasonable grounds, object to a Subprocessor by notifying XXXXXX in writing within 10 days of receipt of XXXXXX's notification, giving reasons for Client's objection. Upon receiving such objection, XXXXXX shall: (a) work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Subprocessor; and (b) where such change cannot be made within 10 days of XXXXXX's receipt of Client's notice, Client may by written notice to XXXXXX with immediate effect terminate the portion of the Agreement or relevant SOW to the extent that it relates to the Services which require the use of the proposed Subprocessor. This termination right is Client's sole and exclusive remedy to Client's objection of any Subprocessor appointed by XXXXXX. XXXXXX shall require all Subprocessors to enter into an agreement with equivalent effect to the Processing terms contained in this Addendum.

Commented [LN8]: You may encounter language from a processor that addresses charging Controller for time spent assisting Controller with meeting its obligations. GDPR does not require reimbursement to the processor – it only requires that the agreement require the processor to assist. Processors may try to insert language such as: "provided that XXXXXX may charge Client on a time and materials basis in the event that XXXXXX considers, in its reasonable discretion, that such assistance is onerous, complex, frequent, or time consuming." Whether to accept the language is a business decision as it is not required by nor prohibited by GDPR.

9. Personal Data Breach. In the event of a Personal Data Breach, XXXXXX will notify Client without undue delay after becoming aware of the Personal Data Breach. Such notification may be delivered to an email address provided by Client or by direct communication (for example, by phone call or an in-person meeting). Client is solely responsible for ensuring that the appropriate notification contact details are current and valid. XXXXXX will immediately provide Client with information available to XXXXXX that Client may require to comply with its obligations as Controller to notify Impacted Data Subjects or Supervisory Authorities.

10. Data Protection Impact Assessment and Prior Consultation. In the event that Client considers that the Processing of Client Personal Data requires a privacy impact assessment to be undertaken or requires assistance with any prior consultations to any Supervisory Authority of Client, following a written request from Client, XXXXXX shall provide relevant information and assistance to Client to fulfill such request.

11. Deletion or Return of Client Personal Data. Unless otherwise required by applicable Data Protection Laws, upon termination or expiration of the MSA or earlier upon request by Client, XXXXXX shall, at Client's option, delete or return all Client Personal Data and all copies to Client within ___ days.

12. Relevant Records and Audit Rights. XXXXXX shall make available to Client on request all information reasonably necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections by Client or an auditor mandated by Client, not being competitors of XXXXXX ("Mandated Auditor") of any premises where the Processing of Client Personal Data takes place. In order to assess compliance with this DPA, XXXXXX shall cooperate with Client in respect of any such audit and shall at the request of Client, provide Client with relevant records of compliance with its obligations under this DPA. XXXXXX shall promptly inform Client if, in its opinion, a request infringes the Data Protection Laws or any other confidentially obligations with XXXXXX's other clients.

13. Restricted Transfer.
    13.1. In the event that any Client transfers any Client Personal Data to XXXXXX in a country outside the EEA, Client on behalf of itself and each Client Affiliate as data exporter and XXXXXX on behalf of itself and each XXXXXX Affiliate as data importer hereby enter into the Standard Contractual Clauses, which terms shall take precedence over those in this DPA. In the event that the Standard Contractual Clauses cease to be recognized as a legitimate basis for the transfer of Personal Data to an entity located outside the EEA, Client shall cooperate with XXXXXX to identify and implement an alternative legitimate basis to the extent that one is required by the Data Protection Laws.
    13.2. The Standard Contractual Clauses shall come into effect on the later of:
        13.2.1. the data exporter becoming party to them;
        13.2.2. the data importer becoming a party to them; and
        13.2.3. commencement of the relevant Restricted Transfer.
    13.3. Section 13.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

Commented [LN9]: You may encounter language from a processor that addresses charging Controller for time spent assisting Controller with meeting its obligations. GDPR does not require reimbursement to the processor – it only requires that the agreement require the processor to assist. Processors may try to insert language such as: "provided that XXXXXX may charge Client on a time and materials basis in the event that XXXXXX considers, in its reasonable discretion, that such assistance is onerous, complex, frequent, or time consuming." Whether to accept the language is a business decision as it is not required by nor prohibited by GDPR.

Commented [LN10]: You may encounter language from a processor that seeks to further define or limit the audit rights/function. Sample language that you may be presented with: "Client agrees that: (a) audits may only occur during normal business hours, and where possible only after reasonable notice to XXXXXX (not less than 20 days' advance notice); (b) audits will be conducted In a manner that does not have any adverse Impact on XXXXXX's normal business operations; (c) Mandated Auditor will comply with XXXXXX's standard safety, confidentiality, and security procedures in conducting any such audits; and (d) any records, data, or information accessed by Mandated Auditor in the performance of any such audit will be deemed to be the Confidential Information of XXXXXX. To the extent any such audit incurs in excess of 20 hours of XXXXXX personnel time, XXXXXX may charge Client on a time and materials basis for any such excess hours."

Again, whether to accept this is a business decision, not a legal one.

Commented [LN11]: See Below for Standard Contractual Clauses template to be included with DPA if Restricted Transfer is involved

Commented [LN12]: If the processor is a member of the U.S. Privacy Shield and that would provide the justification for the transfer, it can and should be added as a separate provision to this section of the contract. Sample language: "XXXXXX and its Affiliates are self-certified to the ELI-U.S. Privacy Shield Framework maintained by the U.S. Department of Commerce and will remain certified for the term of the Agreement provided that the Privacy Shield is recognized by the European Commission as a legitimate basis for the transfer of Personal Data to an entity located In the United States."

14. General Terms. Any obligation imposed on XXXXXX under this DPA in relation to the Processing of Personal Data shall survive any termination or expiration of this Addendum. To the extent that Data Protection Laws do not apply to the Processing of Client Personal Data, this DPA shall be governed by the governing law of the MSA. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either: (a) amended as necessary to ensure its validity and enforceability, while preserving the intent of the provision as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein. With regard to the subject matter of this DPA, the provisions of this DPA shall prevail over the MSA with regard to data protection obligations for Personal Data of a Data Subject under Data Protection Laws.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the MSA with effect from the DPA
Effective Date first set out above.

XXXXXX

Signature

Printed Name

Date

Board of Regents for UW System, UW-Madison

Signature

Printed Name

Date

Standard Contractual Clauses (controller to processor)

Commented [LN13]: For restricted transfers, these are the approved Standard Contractual Clauses for transfer from a Controller to a Processor that serve as the appropriate safeguard that justifies the transfer of personal data outside the EEA. These terms cannot be amended or the appropriate safeguard and justification is lost.

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Between

(hereinafter the "data exporter")

And

(hereinafter the "data importer")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in **Annex A**.

Clause 1 - Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.]

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words "and who is not

subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.]

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 - Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in **Annex A** which forms an integral part of the Clauses.

Clause 3 - Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become

insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4 - Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 - Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented technical organizational and security measures before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 - Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce

its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7 - Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 - Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9 - Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10 - Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 - Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12 - Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

_____
Place, date

_____ _____
Printed Name
Title

On behalf of the importer

_____
Place, date

_____ _____
Printed Name
Title

Annex A (to the Standard Contractual Clauses)

DETAILS REGARDING THE DATA TRANSFER

This Annex forms an integral part of the clauses and any amendments thereto shall require written form.

Data exporter
The data exporter is:
[UNIVERSITY]

Data importer
The data importer is:
[ ]

Data subjects
The personal data transferred concern the following categories of data subjects:
[ ]

Categories of data
The personal data transferred concern the following categories of data:

Processing operations
The personal data transferred will be subject to the following basic processing activities:
[ ]

DATA EXPORTER
[Populated with details of, and deemed to be signed on behalf of, the data exporter:]