Florida State University
INFORMATION SECURITY and
PRIVACY
Standard Terms and Conditions
June 2018

These Information Security and Privacy terms and conditions are hereby incorporated in and attached to Agreements or Contract by and between Florida State University Board of Trustees (University) and **Contractor** by reference. **Contractor** agrees to include all of the terms and conditions contained in this URL in all subcontractor or agency contracts providing services under said Contract.

Contractor acknowledges that its performance of Services under the Contract may involve access to confidential University information including, but not limited to, personally identifiable information, student education records, protected health information, or individual financial information (collectively, "Protected or Private Information as noted in the University's Information Classification Guidelines") that is subject to state, federal, European law/rules/regulations restricting the use and disclosure of such information, including the current versions of:

1) Gramm-Leach-Bliley Act (GLB) (15 U.S.C. §§ 6801(b) and 6805(b)(2)) (Select Student Aid Data);
2) Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) (Select Student Record Data);
3) Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub.L. 104–191, 110 Stat. 1936a) (Select Personal Health Information for university covered components or university holders of a Business Associates Agreement);
4) Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (Select Personal Health Information for university covered components or university holders of a Business Associates Agreement);
5) Payment Card Industry Data Security Standard (PCI DSS) (Select Credit Card Data);
6) International Traffic in Arms Regulations (ITAR) (Select Research Data);
7) Export Administration Regulations (EAR) (Select Research Data);
8) Controlled Unclassified Information in Nonfederal Systems and Organizations NIST Special Publication 800-171;
9) Federal Trade Commission Red Flags Rule (Select Financial Data);
10) European General Data Protection Regulation (GDPR) (EU 2016/679) (Select Data Obtained by Persons in the European Union) (See Appendix A for further GDPR addendum requirements should GDPR protected information be identified and processed under the terms of the master agreement);
11) Florida Information Protection Act, Florida Statute 501.171 Security of confidential personal information.

Contractor agrees to apply and maintain the required safeguarding, privacy, and breach response controls to match the type of "Protected or Private" information transferred or collected on behave of the university to fulfill contracted services.

Contractor agrees to include all of the terms and conditions contained in all subcontractor or agency contracts providing services under this Agreement.

Contractor shall not use, access, or disclose University information in any manner that would constitute a violation of state or federal law or contract or agreement terms including, without limitation, by means of outsourcing, sharing, retransfer, access, or use—to any person or entity, except:

a. Employees or agents who actually and legitimately need to access or use University Data in the performance of **Contractor's** duties under this Agreement or the Contract;

b. Such third parties, such as but not limited to, subcontractors, as may be specifically identified in this Agreement or the Contract, but only after such third party has agreed in writing and in advance of any disclosure, to be bound by all of the terms of this Agreement;

c. Any other third party approved by the University in writing and in advance of any disclosure, but only to the extent of such approval.

I. COMPLIANCE WITH FAIR INFORMATION PRACTICE PRINCIPLES

With respect to the University's Protected or Private Information, and in compliance with all applicable laws and regulations, **Contractor** shall comply in all respects reasonably pertinent to the Agreement with the *Fair Information Practice Principles*, as defined by the U.S. Federal Trade Commission (https://www.ftc.gov/). If collecting Protected or Private Information electronically from individuals on behalf of the University, **Contractor** shall utilize a privacy statement or notice in conformance with such principles (the University's sample Privacy Statement for websites is available at http://fsu.edu/misc/policy.html).

II. PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED INFORMATION

Contractor agrees to hold the University's Protected or Private Information, and any information derived from such information, in strictest confidence. **Contractor** shall not access, use or disclose Protected or Private Information except as permitted or required by the Agreement or as otherwise authorized in writing by University, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected of Private Information, **Contractor** will notify University in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give University an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Any transmission, transportation or storage of Protected or Private

Information outside the United States is prohibited except on prior written authorization by the University.

III. SAFEGUARD STANDARD

Contractor agrees to protect the privacy and security of University data designated as Protected or Private Information in full compliance with any and all applicable laws, regulations, rules or standards, including, but without limitation, FERPA, HIPAA, GLB, the Federal Trade Commission Red Flags Rule, EAR, ITAR, the Social Security Act, and the PCI DSS. **Contractor** shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality (authorized access), integrity and availability of the Protected or Private Information. While **Contractor** has responsibility for the Protected or Private Information under the terms of this agreement, **Contractor** shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities.

Contractor shall not store or process University Protected or Private Information outside of data centers located in the United States without the express prior written approval of the University.

- All facilities used to store and process Protected or Private Information will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure **Contractor's** own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

- Without limiting the foregoing, **Contractor** warrants that all Protected or Private Information will be encrypted in transmission (including via web interface) and may require encrypted storage at no less than 128-bit level encryption.

- **Contractor** will use industry standard and up---to---date security tools and technologies such as antivirus protections and intrusion detection methods in providing Services under this Agreement.

- **If Contractor** is storing, processing, or transmitting cardholder data, or is accepting sensitive authentication data, as defined by the **PCI DSS**, **Contractor** agrees to maintain compliance with the current effective version of the PCI DSS throughout the term of the Agreement or Contract with the University. Upon request by the University, **Contractor** will provide a current PCI DSS Attestation of Compliance.

- If **Contractor** is utilizing a Payment Card Industry Security Standards Council (PCI SSC) approved Point-to-Point Encryption (P2PE) solution to accept or process credit card payments, **Contractor** is responsible for the solution's proper implementation and

operation in compliance with all applicable **PCI DSS** and PCI SSC requirements. Upon request by the University, **Contractor** will provide a current P2PE Instruction Manual, and P2PE Report on Validation (ROV) for the Solution, Application and Components being utilized.

- If **Contractor** is utilizing a University-approved third-party vendor P2PE or End-to-End Encryption solution to accept or process credit card payments, **Contractor** is responsible for the solution's proper implementation and operation in compliance with all applicable PCI DSS, PCI SSC and third-party vendor solution requirements throughout the term of the Agreement or Contract with the University.

- If **Contractor** is utilizing a payment application that is Payment Application Data Security Standard (PA-DSS) validated, **Contractor** is responsible for maintaining its PA-DSS compliance status throughout the term of the Agreement or Contract with the University. Upon request by the University, **Contractor** will provide a current PA-DSS Report on Validation certifying the PA-DSS compliance status of the payment application.

IV. RETURN OR DESTRUCTION OF PROTECTED INFORMATION

Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, **Contractor** shall return the Protected or Private Information to University in an agreed upon format, unless the University requests in writing that such data be destroyed. This provision shall also apply to all Protected or Private Information that is in the possession of subcontractors or agents of **Contractor**. Such destruction shall be accomplished by "purging" or "physical destruction" in accordance with commercially reasonably standards for the type of data being destroyed (e.g., *Guidelines for Media Sanitization*, NIST SP 800---88). **Contractor** shall certify in writing to University that such return or destruction has been completed.

V. BREACHES OF PROTECTED INFORMATION

Definition. For purposes of this article, the term, "Breach," has the meaning given to it under the applicable Florida (F.S. 501.171), applicable state or federal rule/regulation, or contractual obligation.

Reporting of Breach.

1) Gramm-Leach-Bliley Act (GLB) (15 U.S.C. §§ 6801(b) and 6805(b)(2)) (Select Student Aid Data)-**Contractor must report any "suspected" data breach on the day it is detected**;

2) Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) (Select Student Record Data)-**Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than **two (2) business days** after **Contractor**

knows or reasonably suspects a Breach has or may have occurred;

3) Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub.L. 104–191, 110 Stat. 1936a) (Select Personal Health Information for university covered components or university holders of a Business Associates Agreement)- **Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than **two (2) business days** after **Contractor** knows or reasonably suspects a Breach has or may have occurred;

4) **Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009** (Select Personal Health Information for university covered components or university holders of a Business Associates Agreement)- **Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than **two (2) business days** after **Contractor** knows or reasonably suspects a Breach has or may have occurred;

5) **Payment Card Industry Data Security Standard (PCI DSS)**(Credit Card Data)- **Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than **one (1) day** after **Contractor** knows or reasonably suspects a Breach has or may have occurred;

6) **International Traffic in Arms Regulations (ITAR)** (Select Research Data)-**Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than **two (2) business days** after **Contractor** knows or reasonably suspects a Breach has or may have occurred;

7) **Export Administration Regulations (EAR)** (Select Research Data)- **Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than **two (2) business days** after **Contractor** knows or reasonably suspects a Breach has or may have occurred;

8) **Controlled Unclassified Information in Nonfederal Systems and Organizations NIST Special Publication 800-171** (Select Research Data)- **Contractor** shall report both orally and in writing to the University. The report should be made more within **one (1) day** after **Contractor** knows or reasonably suspects a breach has or may have occurred;

9) **Federal Trade Commission Red Flags Rule** (Select Financial Data)- **Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than **two (2) business days** after **Contractor** knows or reasonably suspects a Breach has or may have occurred;

10) **European General Data Protection Regulation (GDPR)** (EU 2016/679) (Select Data Obtained by Persons in the European Union and Switzerland) (See Appendix A for further GDPR addendum requirements)- The processor shall notify the controller

without undue delay after becoming aware of a personal data breach (Article 33 GDPR);

11) **Florida Information Protection Act, Florida Statute 501.171** Security of confidential personal information- **Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than **two (2) business days** after **Contractor** knows or reasonably suspects a Breach has or may have occurred.

Contractor shall keep the University informed regularly of the progress of its investigation until the uncertainty of the breach event is resolved.

Contractor's report shall identify:

(i) The nature of the unauthorized access, use or disclosure,
(ii) The Protected or Private Information accessed, used or disclosed,
(iii) The person(s) who accessed, used and disclosed and/or received Protected or Private Information (if known),
(iv) What **Contractor** has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and
(v) What corrective action **Contractor** has taken or will take to prevent future unauthorized access, use or disclosure.
(vi) **Contractor** shall provide such other information, including a written report, as reasonably requested by University.

Coordination of Breach Response Activities. In the event of a Breach, **Contractor** will:

• Immediately preserve any potential forensic evidence relating to the breach;
• Promptly designate a contact person to whom the University will direct inquiries, and who will communicate **Contractor** responses to University inquiries;
• As rapidly as circumstances permit, apply appropriate resources to remedy the breach condition, investigate, document, restore University service(s) as directed by the University, and undertake appropriate response activities;
• Provide status reports to the University on Breach response activities, either on a daily basis or a frequency approved by the University;
• Coordinate all media, law enforcement, or other Breach notifications with the University in advance of such notification(s), unless expressly prohibited by law;
• Make all reasonable efforts to assist and cooperate with the University in its Breach response efforts; and
• Ensure that knowledgeable **Contractor** staff are available on short notice, if needed, to participate in University---initiated meetings and/or conference calls regarding the Breach.

Costs Arising from Breach. In the event of a Breach by the **Contractor** or its staff, **Contractor** agrees to indemnify and hold harmless the University arising from such Breach, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of University personnel responding to Breach, civil or criminal penalties levied against the University, attorney's fees, court costs, etc. Any Breach may be grounds for immediate termination of this Agreement by the University.

VI. EXAMINATION OF RECORDS

University shall have reasonable access to and the right to examine any pertinent books, documents, papers, and records, regardless of the records' format, of **Contractor** involving transactions and work related to this agreement until the expiration of five years after final payment hereunder. **Contractor** shall retain project records for a period of five years from the date of final payment.

VII. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

Contractor shall make itself and any employees, subcontractors, or agents assisting **Contractor** in the performance of its obligations under the Agreement available to University at no cost to University to testify as witnesses in the event of an unauthorized disclosure caused by **Contractor** that results in litigation or administrative proceedings against University, its directors, officers, agents or employees based upon a claimed violation of laws relating to security, privacy or arising out of this agreement.

VIII. SURVIVAL

Contractor shall maintain an industry standard disaster recovery program to reduce in potential effect of outages because of supporting data center outages. Any backup site used to store
University Protected or Private data will include the same information security and privacy controls as the primary data center(s).

In the event of termination of the Contract, for any reason, sections V, VI, and VII shall survive for a minimum of five years from the date of such termination.

IX. RIGHT TO AUDIT

Contractor agrees that, as required by applicable state and federal law, auditors from state, federal, Florida State University, or other agencies so designated by the State or University, shall have the option to audit the outsourced service. Records pertaining to the service shall be made available to auditors and the University during normal working hours for this purpose.

Appendix A - General Data Protection Regulation Provisions

Processing in accordance with Article 28 General Data Protection Regulation (GDPR)

[as of: May 2017]

Agreement

between

.....Florida State University.....

– the Controller – hereinafter referred to as the Data Controller -

and

.....Contractor.....

– the Processor - hereinafter referred to as the Data Processor

[When applicable: Authorised Representative in accordance with Article 27 GDPR:

.....]

1. **Definitions.**

(a) "EEA Personal Data" means personal data (as defined in GDPR) pertaining to information received from individuals within the European Economic Area (EEA) and Switzerland;

(b) "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation and by association the Swiss Data Protection Act (DPA);

(c) "Internal Control Report" means a Type II Service Organizational Control (SOC) report (based on the SSAE 18 Attestation Standards: Clarification and Recodification or ISAE 3402 model) or any successor report thereto;

(d) "Personal Information" means any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. Personal Information includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data, "personal data" (as defined in the GDPR) and any and all information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person's online activities,

browsing, application or hotspot usage or device location. Personal Information includes data either received into the contractor's systems from an IP addresses located within the European Economic Area and Switzerland or as designated as EEA Personal Data from university information processing assets transfers;

(e) "Privacy Laws" means all applicable U.S. and international laws that regulate the Processing of Personal Information. In particular, "Privacy Laws" includes those listed in the introductory paragraph of this document including GDPR that specify privacy, security or security breach notification obligations that affect the Personal Information or the provision of the services by **Contractor**;

(f) "Processing" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, Transfer, transmission, combination, redaction, erasure, or destruction;

(g) "Security Breach" means a "personal data breach" (as defined in the GDPR), a "breach of the security of a system" or similar term (as defined in any other applicable Privacy Law or any other event that compromises the security, confidentiality or integrity of Personal Information;

(h) "Sensitive Personal Information" is a subset of Personal Information, which due to its nature has been classified by law or by the university policy as deserving additional privacy and security protections. Sensitive Personal Information includes Special Categories of Data under the GDPR, namely EEA Personal Data revealing 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;

(i) "Services" means any and all services that the university requests the **Contractor** to perform under the Standard Terms and Conditions or any other contract or agreement that involves Processing of Personal Information;

(j) "Data Controller" means the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. The university or specific designated employees of the university are considered "Controller's" under this agreement;

(k) "Data Processor" means a natural or legal person, public authority, agency or other body (**Contractor**) which processes personal data on behalf of the controller under this agreement;

(l) "Subprocessor" means any third party (including an affiliate of **Contractor**) that provides any services to **Contractor** and that may have access (including inadvertent access) to any unencrypted university Personal Information;

(m) "Transfer" means to disclose or otherwise make the Personal Information available to a third party (including to any affiliate or Subprocessor of **Contractor**), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

1. Subject matter and duration of the Order or Contract

(1) Subject matter

☐ The Subject matter of the Order or Contract results from the Service Agreement/SLA/ …….. dated ……., which is referred to here (hereinafter referred to as Service Agreement).

or

☐ The Subject matter of the Order or Contract regarding the processing of data is the execution of the following services or tasks by the Data Processor (Definition of the services or tasks)

- Task 1 _____
- Task 2 _____
- Task 3 _____
- Task 4 _____

(2) Duration

☐ The duration of this Order or Contract corresponds to the duration of the Service Agreement.

or (specifically, if no Service Agreement regarding the Duration exists)

☐ The Order or Contract will be authorised for one-time execution only.

or

☐ The Duration of this Contract is limited to …….. .

or

☐ The Contract is authorised for an unlimited period and can be cancelled by either Party with a notice period of……(time period) to …….(deadline) . This does not prejudice the right to termination of the contract without notice.

2. Specification of the Order or Contract Details

(1) Nature and Purpose of the intended Processing of Data

☐ Nature and Purpose of Processing of personal data by the Data Processor for the Data Controller are precisely defined in the Service Agreement dated …… .

or

☐ Detailed description of the Subject Matter with regard to the Nature and Purpose of the services provided by the Data Processor: .....

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within the United States of America. Each and every Transfer of Data requires the prior agreement of the university as the Data Controller.

(2) Type of Data

☐ The type of personal data used is precisely defined in the Service Agreement under:…..

or

☐ The Subject Matter of the processing of personal data comprises the following data types/categories (List/Description of the Data Categories)

- ☐ Personal Master Data (Key Personal Data)
- ☐ Contact Data
- ☐ Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)
- ☐ Customer History
- ☐ Contract Billing and Payments Data
- ☐ Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories...
- ☐ Other:… (Please specify)

(3) Categories of Data Subjects

☐ The Categories of Data Subjects are precisely defined in the Service Agreement under:.....

or

☐ The Categories of Data Subjects comprise:

- ☐ Customers
- ☐ Potential Customers
- ☐ Subscribers
- ☐ Employees
- ☐ Data Processors
- ☐ Authorised Agents
- ☐ Contact Persons
- ☐ Other:…… (Please specify)

3. Technical and Organizational Measures

(1) Before the commencement of processing, the Data Processor shall document the execution of the necessary Technical and organizational measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Data Controller for inspection. Upon acceptance by the Data Controller, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Data Controller shows the need for amendments, such amendments shall be implemented by mutual agreement.

(2) The Data Processor shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account.
(3) The Technical and Organizational Measures are subject to technical progress and further development. In this respect, it is permissible for the Data Processor to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Data Processor may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Data Controller, but only on documented instructions from the Data Controller. Insofar as a Data Subject contacts the Data Processor directly concerning a rectification, erasure, or restriction of processing, the Data Processor will immediately forward the Data Subject's request to the Data Controller.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Data Processor in accordance with documented instructions from the Data Controller without undue delay.

5. Quality assurance and other duties of the Data Processor

In addition to complying with the rules set out in this Order or Contract, the Data Processor shall comply

with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Data Processor ensures, in particular, compliance with the following requirements:

a) ☐ Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR.
   - ☐ The Data Controller shall be informed of his/her contact details for the purpose of direct contact. The Data Controller shall be informed immediately of any change of Data Protection Officer.
   - ☐ The Data Processor has appointed Mr/Ms [enter: given name, surname, organizational unit, telephone, e-mail] as Data Protection Officer. The Data Controller shall be informed immediately of any change of Data Protection Officer.
   - ☐ His/Her current contact details are always available and easily accessible on the website of the Data Processor.

b) ☐ The Data Processor is not obliged to appoint a Data Protection Officer. Mr/Ms [enter: given name, surname, organizational unit, telephone, e-mail] is designated as the Contact Person on behalf of the Data Processor.

c) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Data Processor entrusts only such employees with the data processing outlined in this Terms and Conditions who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Data Processor and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Data Controller, which includes the powers granted in this Terms and Conditions, unless required to do so by law.

d) Implementation of and compliance with all technical and organizational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Appendix B].

e) The Data Controller and the Data Processor shall cooperate, on request, with the supervisory authority in performance of its tasks.

f) The Data Controller shall be informed immediately of any inspections and measures conducted by a EU member state supervisory authority (Defined in Article 51 GDPR), insofar as they relate to this Order or Contract. This also applies insofar as the Data Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this Order or Contract.

g) Insofar as the Data Controller is subject to an inspection by an EU member supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract data processing by the Data Processor, the Data Processor shall make every effort to support the Data Controller.

h) The Data Processor shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within their area of responsibility is in

accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.

i) Verifiability of the Technical and Organizational Measures {Appendix B} conducted by the Data Controller as part of the Data Controller's supervisory powers referred to in item 7 of this Terms and Conditions.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Data Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Data Controller's data, even in the case of outsourced ancillary services.

(2) The Data Processor may commission subcontractors (additional contract processors) only after prior explicit written or documented consent from the Data Controller.

a) ☐ Subcontracting is not permitted.

b) ☐ The Data Controller agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

Company subcontractor	Address/country	Service

c) ☐ Outsourcing to subcontractors or

☐ Changing the existing subcontractor

are permissible when:

- The Data Processor submits such an outsourcing to a subcontractor to the Data Controller in writing or in text form with appropriate advance notice; and
- The Data Controller has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Data Processor; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Data Controller to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) Further outsourcing by the subcontractor

☐ Is not permitted;

☐ Requires the express consent of the main Data Controller (at the minimum in text form);

☐ Requires the express consent of the Data Processor (at the minimum in text form);

All contractual provisions in the contract chain shall be communicated to and agreed with each and every

additional subcontractor.

7. Supervisory powers of the Data Controller

(1) The Data Controller has the right, after consultation with the Data Processor, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Data Processor in his business operations by means of random checks, which are ordinarily to be announced and agreed by both Contractor and the university.

(2) The Data Processor shall ensure that the Data Controller is able to verify compliance with the obligations of the Data Processor in accordance with Article 28 GDPR**.** The Data Processor undertakes to give the Data Controller the necessary information on request and, in particular, to demonstrate the execution of the technical and organizational Measures {Appendix B}.

(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

- ☐ Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
- ☐ Certification according to an approved certification procedure in accordance with Article 42 GDPR;
- ☐ 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)

(4) The Data Processor may claim remuneration for enabling Data Controller inspections.

8. Communication in the case of infringements by the Data Processor

(1) The Data Processor shall assist the Data Controller in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through Technical and Organizational Measures {Appendix B} that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
b) The obligation to report the confirmation of a personal data breach within 24 hours to the Data Controller
c) The duty to assist the Data Controller with regard to the Data Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Data Controller with all relevant information in this regard.
d) Supporting the Data Controller with its data protection impact assessment
e) Supporting the Data Controller with regard to prior consultation of the supervisory authority

9. Authority of the Data Controller to issue instructions

(1) The Data Controller shall immediately confirm oral instructions (at the minimum in text form).

(2) The Data Processor shall inform the Data Controller immediately if he considers that an instruction violates Data Protection Regulations. The Data Processor shall then be entitled to suspend the execution of the relevant instructions until the Data Controller confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Data Controller, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Data Controller, at the latest upon termination of the Service Agreement, the Data Processor shall hand over to the Data Controller or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.
(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Data Processor in accordance with the respective retention periods. It may hand such documentation over to the Data Controller at the end of the contract duration to relieve the Data Processor of this contractual obligation.

Appendix B - Technical and Organizational Measures Detail

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- Physical Access Control
  No unauthorized access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
- Electronic Access Control
  No unauthorized use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)
  No unauthorized Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorization concept, need-based rights of access, logging of system access events
- Isolation Control
  The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Data Controller support, sandboxing;
- Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
  The processing of personal data in such a method/way, that the data cannot be associated with a specific Data Subject without the assistance of additional Information, provided that this additional information is stored separately, and is subject to appropriate Technical and Organizational Measures.

2. Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control
  No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;
- Data Entry Control
  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management

3. Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control
  Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR);

4. Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);
- Order or Contract Control
  No third party data processing as per Article 28 GDPR without corresponding instructions from the Data Controller, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.