American University of Malta
Policy: 2019.xx.v1-QA-Po
AUM Policy Category: Quality Assurance

Policy Title	GDPR
Policy ID	2019. 99-vl-QA_Po
Effective Date	January 21, 2019
Last updated	January 21, 2019
Responsible Office	Human Resources
Responsible Executive(s)	Vice President of Administrative Affairs

Rationale: The American University of Malta and Sadeen Education Investments Limited ("AUM") are committed to complying with the EU General Data Protection Regulation and the Data Protection Act, 2018 (collectively referred to as "data protection laws") in relation to the collection, handling and processing of personal data. Sadeen Education Investments Limited, as data controller, collects, handles and stores personal data relating to individuals which include student and job applicants, present and former students, present and former employees, website users, contractors and other contacts. In this respect it has a responsibility to implement and comply with data protection laws.

This policy sets out how AUM manages its duties and responsibilities in accordance with data protection laws as an academic institution, an employer and as a service provider. It seeks to ensure that AUM:

i. processes personal data fairly, lawfully and in a transparent manner in accordance with the personal data protection principles;
ii. integrates data protection principles into its processing activities from design stage;
iii. only processes the data that is necessary to achieve its specific purpose;
iv. supports the data protection rights of individuals; and
v. implements effective security measures at all times.

Scope:

Data Controller	The person who determines the purposes and means of the processing of personal data
Data Processor	Any individual or organization who processes personal data on behalf of the data controller.
Personal data	Any information relating to an identified or identifiable natural person
Processing	Any operation which is performed on personal data such as collection, storage, use and erasure
Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic and biometric data and data concerning health, sex life or sexual orientation

This policy applies in all cases where AUM is the data controller or data processor of personal data, regardless of who created the data and where it is stored. In these cases; it applies to all employees and students who process such personal data. Disciplinary action may be taken as a result of non-compliance with this policy.

AUM will appoint a Data Protection Representative to who shall serve as the contact person in relation to data protection matters.

Policy:

1.The duty to comply with the Data Protection Principles

AUM must adhere to, and be able to demonstrate, compliance with the Data Protection Principles, outlined hereunder, when it determines the purposes for which, and the manner in which, personal data is to be or is processed.

Lawfulness, fairness and transparency
AUM must ensure that personal data is processed lawfully, fairly and in a transparent manner. It explains to its applicants, students and employees how, the legal basis and for what purposes it processes their personal data at the time of collection. The relevant Privacy Notices should be made available at the time of collection of personal data.

Purpose Limitation
AUM should only collect and specified, explicit and legitimate purposes and use it only for such purposes.

Data minimisation
AUM should limit the collection and handling of data only to what is necessary in relation to the purposes for which it is required for.

Accuracy
AUM should ensure that the personal data it holds is accurate and up to date. It should also make sure that any mistakes may be easily rectified and without delay.

Storage Limitation
AUM should ensure that personal data is not held for no longer than is necessary.

Integrity and Confidentiality
AUM should ensure that appropriate security measures are implemented to safeguard unlawful access, loss or destruction of personal data.

Accountability

AUM is responsible for and should ensure that it has appropriate processes and records in place to demonstrate compliance with all of the above Data Protection Principles.
AUM must make sure that it has the necessary resources and adequate controls to ensure and document compliance with all of the above principles. To demonstrate our compliance with these principles we should ensure that we implement the following measures:

i. adopt and implement data protection policies;
ii. take a 'data protection by design and default' approach, and therefore implement privacy during the design stage and completing a Data Protection Impact Assessment (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests;
iii. put written contracts in place with organisations that process personal data on our behalf;
iv. maintain documentation of our processing activities;
v. implement appropriate security measures;
vi. record and, where necessary, report personal data breaches;
vii. appoint a data protection officer or where this is not compulsory appoint a data protection representative who will be the ultimate point of contact for all data protection matters;
viii. train staff on data protection laws on a regular basis and keeping a record thereof; and
ix. regularly test the privacy measures that have been implemented and assess their adequacy by using the results to identify how we may improve such measures.

2. Legal basis for processing

AUM must ensure that it meets one of the six lawful bases under Article 6 of the GDPR before it processes personal data and should document it. AUM should also ensure that it selects the most appropriate lawful basis or bases for each activity. The most common legal bases are set out below:

Necessary for the performance of a contract

The processing of most of the personal data of our students and employees is necessary for the performance of a contract we have with them, or in the case of applicants, it is necessary to take necessary steps upon their request prior to entering the contract with them.

Necessary for the performance of a legal obligation

The processing of certain personal data of our students and employees is necessary for us to comply with the various laws, including laws regulating academic institutions, employment, social security and tax.

Consent

AUM would normally require consent in relation to optional services offered to our students, employees and customers.

Necessary for our legitimate interests
AUM may process personal data of applicants, students, employees and customers where this is necessary for our legitimate interests or the legitimate interests of a third party unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Processing under this ground covers CCTV surveillance for security purposes.

3. *Special Category Data*

AUM should ensure to identify at least one lawful basis for processing and a special category condition for processing. It should also document both the lawful basis and the special category condition, under Article 9 of the GDPR, to demonstrate compliance and accountability.

The following is a summary of the conditions listed in Article 9 of the GDPR:

Explicit consent
The data subject has given explicit consent to the processing of the personal data for specified purpose/s.

Necessary for certain specific purposes
The processing is necessary for the purposes of employment, social security and social protection law.

Necessary for the protection of the vital interests of data subject
The processing is necessary to protect the vital interests of the data subject or of another natural person whether he/she is physically or legally incapable of giving consent.

Processing by a not-for-profit body
The processing is carried out by a not-for-profit body in the course of its legitimate activities and on condition that the processing relates solely to its members or former members.

Processing manifestly made public
The processing relates to personal data which is manifestly made public by the data subject.

Processing necessary for legal claims
The processing is necessary for the establishment or defence of legal claims.

Processing is necessary for reasons of substantial public interest
The processing is necessary for reasons of substantial public interest, on the basis of EU or national law which is proportionate to the aim pursued.

Processing is necessary for purposes of medicine
The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of heath or social care or treatment or the management of health or social care systems and services.

Processing is necessary for public health
The processing is necessary for reasons of public interest in the area of public health.

Processing is necessary for archiving purposes
The processing is necessary for the archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards.

4. Data Subject Rights

Data subjects have a number of rights under the data protection laws. AUM shall ensure that it respects the rights of its students, employees and customers when it processes their personal data. These rights include:

Right to information
Data subjects have the right to be informed about the collection and use of their personal data. Please refer to the specific Privacy Notices.

Right of Access
Data subjects have the right to access and be provided with a copy of their personal data. AUM shall respond within one month of the request.

Right to Rectification
AUM shall use its best endeavours to ensure that the data it processes is accurate. It will take all reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes. Data subjects have the right to require us to correct any inaccurate personal

data about them. We shall respond within one month of the request. We shall assess their request and rectify any inaccuracies.

Right to be forgotten

Data subjects have the right to require us to delete their personal data in certain circumstances. This right is not absolute and AUM shall examine those specific circumstances against each request. AUM shall respond within one month of the request. Some of these circumstances are listed below:

i. the personal data is no longer necessary for the purpose which we originally collected or processed it for.
ii. we rely on the data subject's consent as our lawful basis for holding the data, and the he withdraws his consent.
iii. we rely on legitimate interests as our basis for processing, the individual objects to the processing of his data, and there is no overriding legitimate interest to continue this processing.
iv. we are processing the personal data for direct marketing purposes and the individual objects to that processing.
v. we have processed the personal data unlawfully and therefore in breach of the lawfulness requirement as indicated in the first principle in Section 3 above.
vi. we have to do it to comply with a legal obligation.

Right to restriction of processing

Data subjects have the right to require us to restrict processing their personal data in certain circumstances**.** This right is not absolute and AUM shall examine those specific circumstances against each request. AUM shall respond within one month of the request. Some of these circumstances are listed below:

i. the individual contests the accuracy of his personal data and we are verifying the accuracy of the data.
ii. the data has been unlawfully processed and the individual opposes erasure and requests restriction instead.
iii. you no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim.

Right to data portability

Data subjects have the right to receive their personal data which they provided to us, in a structured, commonly used and machine-readable format and the right to transmit that data to another data controller in certain circumstances. AUM shall respond within one month of the request.

Right to object

Data subjects have the right to object to the processing of their personal data in certain circumstances which include processing for direct marketing purposes and continued processing of their data carried out for the purpose of our legitimate interests. AUM will assess such request and respond accordingly. AUM shall respond within one month of the request.

Right not to be subject to automated processing

Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning them or significantly affects them. AUM does not make decisions about data subjects through purely automated means.

5. Record Keeping

Presently, the data protection laws require AUM (with less than 250 employees) to keep records of its data processing activities which are not occasional or could result in a risk to the rights and freedoms of individuals or involve the processing of special categories of data or criminal conviction and offence data. The staff who process data should keep and maintain accurate records of all our processing activities which relate to the processing of data relating to applicants, students, employees and customers. These records, which must be kept in writing and on the AUM record keeping model, should include:

i. The name and contact details of AUM as the controller (and, where applicable of the data protection officer).
ii. The purposes of our processing.
iii. A description of the categories of individuals, such as students or employees and categories of their personal data.
iv. The categories of recipients of personal data.
v. Information required for processing special category data or criminal conviction and offence data.
vi. Controller-processor contracts
vii. A record of all the consents given to us by individuals, where consent is the legal basis for processing.
viii. Details of your transfers to third countries including documenting the transfer mechanism safeguards in place, where applicable.
ix. Retention schedules.
x. Data Protection Impact Assessment Reports
xi. A description of the technical and organisational security measures in place.
xii. Records of data subject requests
xiii. Records of data protection breaches, setting out the facts surrounding the breach, its effects and the remedial action taken.

6. Data Retention

Data protection laws require that we do not retain personal data for longer than required. AUM may only keep personal data for so long as one of the purposes for processing still applies. We should periodically review the data we hold, and erase or anonymise it when this is no longer necessary.

7. Data Protection by Design and Default

Data protection by design requires AUM to ensure that it makes data protection an essential element of the core functionality of its processing systems. We should seek to anticipate risks and privacy invasive events before they occur and take the necessary steps to prevent a negative impact on the individual's privacy.

Data protection by default requires AUM to ensure that it only process the data that is necessary to achieve its specific purpose.

8. Security

AUM has implemented a comprehensive ICT security policy ensuring that personal data is processed in a manner that ensures appropriate security and protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

9. Responsibilities of Data Users

All Directors and Senior Management personnel are responsible to ensure compliance with the data protection laws and this policy, as well as, to develop and monitor good information handling practices within their areas of responsibility. All other employees who process personal data about student applicants, job applicants, students, employees and any other individuals, including in particular employees who work in the admissions and human resources departments must comply with the requirements of this policy.

9.1 The Data Protection Representative

The Data Protection Representative ("DPR") is the key person responsible for the management of data protection matters and overseeing AUM's compliance with data protection laws. He is the first point of contact for data protection questions coming from all data users. For the avoidance of doubt, the Data Protection Representative is not the equivalent of the Data Protection Officer in terms of the GDPR. He is responsible for:

i. reporting to and keeping the upper management updated about AUM's data protection responsibilities, risks and issues at all times;
ii. reviewing all data protection procedures and policies on a regular basis and keeping them updated;
iii. being the immediate point of contact to data users in relation to all matters relating to data protection and answering in a clear and efficient manner any questions referred to him by AUM or the data users;
iv. receiving and dealing with notifications with respect to data protection incidents;
v. ensuring that data users are adequately trained on data protection laws and responding to training requests;
vi. advising AUM and all data users of their obligations in terms of the data protection laws;
vii. coordinating and/or responding to data subject requests, and
viii. liaising with third parties and professionals, such as AUM's legal advisors, in relation to matters which require input from a professional advisor, such as the review of data processing agreements, policies and procedures in order to make sure that such documents are in compliance with data protection laws.

9.2 The IT Director

The IT Director is responsible for:

i. working in collaboration with the DPR and managing the policies and procedures with the DPR;
ii. examine and report on any risks in the ICT systems to the DPR;
iii. working with the DPR to ensure compliance by the data users of the policies and fix the process in the first priority
iv. ensuring all systems, services, software and equipment are secure in terms of data protection laws and meet the security standards provided in the ICT security policy;
v. checking and scanning security hardware and software regularly to ensure it is functioning properly in terms of data protection laws and the ICT security policy, and
vi. researching third-party services, such as cloud services the company is considering using to store or process data, which are reputable and compliant with data protection laws and to ensure that a data processing agreement in terms of the GDPR is entered into between AUM and such third-party service provider.

9.3 The Marketing Department

Marketing and Business Development Department is responsible for the following:

- working in collaboration and consulting with the DPR in relation to all data protection matters
- responding to data protection queries from prospective students, target audiences or media outlets in accordance with the terms of this policy and, depending on the level and type of the enquiry, after consultation with the DPR.
- coordinating with the DPR to ensure that all marketing/recruitment activities and processes comply with the data protection laws and this policy prior to their implementation.

9.4 The Human Resources Department

The HR Department is responsible for:

- working in collaboration and consulting with the DPR on all data protection matters relating to employees.
- ensuring that employee personal data is accessed only by authorised users.
- ensuring that employee personal data both physical and electronic is stored in a secure environment with restricted access.
- ensuring that employee personal data is collected and processed in accordance with all applicable data protection laws and policies, including the GDPR.
- responding to data protection queries from employees in accordance with this policy and depending on the level and type of the query, after consultation with the DPR.

9.5 Students

Students are responsible for reading and understanding the Privacy Notice provided when they register with the University and to immediately inform AUM of any changes to the personal data they shared with it.

10. Sharing Personal Data

Personal data should not be shared with third parties unless consent has been obtained or upon satisfaction of one of the legal bases for processing. It is also permitted to share data with authorities who have a statutory power to obtain information. However, the person receiving the request should inform the DPR of such request and verify whether that authority or legal entity has such power before disclosing the requested information.

11. Transfers of Personal Data Outside the EEA

Transfers of personal data outside the EEA are subject to data protection laws. Any transfer of personal data may only be made where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

12. Direct Marketing

Direct marketing is the promotion of aims and ideals as well as the sale of products and services.

AUM must ensure that it obtains consent of its applicants, students, or other person requesting our services prior to sending out any marketing material via electronic means, such as by email or text messages.

Individuals receiving such marketing material should always be given the opportunity to object to direct marketing by giving them the opportunity to do so in a clear and intelligible manner. Objections by any individuals should be immediately honoured. In the event that an individual opts out, AUM should suppress his/her details, without delay, to the extent to ensure that his/her marketing preferences are respected from thereon.

13. Audits

AUM shall ensure that data audits for the purposes of managing and mitigating data protection risks are performed periodically and when deemed necessary.

14. Training

AUM will ensure that all AUM staff have the requisite training and awareness to enable them to comply with data protection laws and this policy. Any data user who may require any further training should contact the DPR.

Any breach of data protection laws and/or this policy by a data user or other member of staff, may result in disciplinary action, up to and including dismissal.

Personal Data Breaches & Reporting

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. Examples include access by an unauthorised third party, sending personal data to an incorrect recipient, alteration of personal data without permission and loss of availability of personal data. AUM makes every effort to avoid incidents causing a personal data breach, however, it is possible that mistakes occur at some point in time.

In the event of a security incident, AUM is required to establish, without delay, whether a personal breach has occurred and, if so, promptly take steps to address it, including informing the DPR.

Data protection laws require AUM to report breaches, that are likely to result in a risk to an individual/s rights and freedoms, to the Office of the Information and Data Protection Commissioner ("IDCP"). If it is unlikely that a breach will affect the rights and freedoms of individuals then AUM is not required to notify the IDCP.

If a personal data protection incident occurs, it must be brought to the attention of the DPR immediately, who will in conjunction with senior management decide whether it constitutes a reportable data protection breach. In such case, AUM should report the breach to the IDCP by not later than 72 hours after becoming aware of it.

AUM is required to immediately inform the DPR of anything you may consider to be a data protection incident, by email which should be tagged as urgent and with "GDPR incident" in the subject line.