AUM
AMERICAN UNIVERSITY OF MALTA

Information Management Policy

Last review: July 2021
Published: August 2021

Contents

Data protection policy

1.Policy statement

As an academic institution, an employer, and a service provider, the University is dedicated to complying to the General Data Protection Regulation. In order to do this, the University agrees to:

- We process our data in a fair and lawful manner.
- We believe in the rights of individuals.
- We safeguard our personal information.
- We include privacy into our systems and procedures.

2.Scope

The University is subject to the General Data Protection Regulation and associated data protection legislation. The University covers the University's central academic activities, administrative functions, libraries and business services.

3.Definitions

The General Data Protection Regulation governs the processing of personal data. The following definitions are used:

- **Personal data** are data which can identify living individuals. As well as images, names and contact details it can also include numerical or statistical information from which an individual's identity can be derived.
- A **Data Subject** is the individual who is the subject of personal data.

4.Principles

The University is required to process personal data according to the following six principles:

Data Protection Principles	**The context for the University**
Lawfulness, fairness and transparency	The University explains to its staff, students and customers how it processes personal data at the point of collection and for what purposes
Purpose limitation	The University only uses the personal data it has for the purposes it was collected for
Data Minimization	The University only collects personal data which is relevant to the purposes it is required for
Accuracy	The University ensures that the data is correct, up to date and be able to rectify any mistakes quickly
Storage Limitation	The University does not retain personal data for longer than it is needed
Integrity and Confidentiality	The University protects its personal data against unauthorized access, loss or destruction by a range of security measures

5.Legal basis for processing – personal data

The University needs to meet the most common following lawful bases in order to process personal data:

Legal basis	Examples for the University
Necessary for the performance of a contract	Covers the majority of processing for our students and staff
Data subject has given consent to the processing	Covers mailing lists, marketing and other optional services for staff, students and customers
Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	Covers the retention of our student pass lists and transcript information for awards and verification
Necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data	Covers activities around alumni, charitable works and marketing of commercial services

6.Rights

Data subjects – our students, staff, and Faculty – have a number of rights under the Regulation. These include:

Right	The context for the University
Right of access	Data subjects have the right to find out about what we are doing with their data, check we are holding it correctly, and obtain a copy of what we hold.
Right to rectification	The University makes every effort to ensure its data is accurate. If a data subject thinks something we hold about them is wrong, And they can ask anytime for this to be corrected. Then, The University will assess the request and correct any
Right to erasure / right to be forgotten	Data subjects have the right to ask us to remove or delete the data we hold on them. The University will assess the request against the criteria and respond accordingly.
Right to restriction of processing	Data subjects may, in the course of a dispute with the University about the use of their data, ask the University to stop using their data if certain criteria apply.
Right to data portability	Data subjects have the right to ask the University to provide them with a re-usable electronic copy of their data to allow them to transfer it to another provider. This only covers data submitted to the University by the subject or data observed from the subject's use of a service If technically possible, the University will consider transferring information directly to another provider.

Right to object	Data subjects have the right to object to processing based on legitimate interests, legal obligation or for the purposes of direct marketing or for "scientific or historical research purposes or statistical purposes". The University will assess the request and respond accordingly.
Automated decision making, including profiling	If the University is making decisions about data subjects through purely automated means, such as a computer algorithm, data subjects can appeal against this decision. The University will ensure that subjects can express their point of view and have member of staff provide a review and explanation of the decision.

7.Data Protection by design

The University is committed to ensuring privacy is built into to its processes and outcomes. New projects involving personal data are required to carry out a privacy impact assessment to identify privacy risks and plan appropriate mitigation.

8.Training and awareness

The University is committed to ensuring its staff has the requisite training and awareness around data protection. All staff must undertake the compulsory ‘Data Protection’ and ‘IT Security training. Further resources and training are provided on the staff intranet and on request from the IT Department.

Backup Policy

1.Desktop and Laptop Backup Policy

Local documents stored on desktop and laptop computers should be backed up so the documents and files can be restored in the event of a physical problem with the machine or if individual files or folders are inadvertently removed.

- University faculty and staff have access to a networked drive provided by Information Technology. Faculty and staff in AUM University may have access to division-specific resources.

- All network storage resources must have a backup policy. Non-IT domains need an IT-approved backup policy for Desktop and Laptop Computers. A current copy of this policy must be on file with IT Individuals using non-IT domains must follow the approved backup policy.

2.Backup Modes

- Network file storage is the main backup mode.

- Files may be copied to once-writeable media (CDs, DVDs) or rewriteable storage media (e.g., hard disks, other magnetic media, and flash memory devices/thumb drives in addition to the Main Data Storage). These media must be stored in a secure location.

- Cloud Backup Storage via Office365 OneDrive

3.Server Backup Policy

Backup procedures and policies are developed for two purposes, disaster recovery and file recovery. In the event of a catastrophe, due to a physical disaster, personnel error, or other misfortune, reliable backups must provide timely and accurate restoration of all functions of the organization. Individual file recovery may be required to restore programs, information, And- or other data that has become corrupted or inadvertently removed.

- Backup procedures for all servers must be approved by IT. Procedures must include an appropriate time schedule, media description, storage, documentation, and testing process.
- Knowledge of the backup location and access to the site should be limited to a few key people within the organization, but at least two individuals should have access to the facility.

All AUM systems and network are fully secured against any attack and violation. We have a firewall system on the premise that protects all AUM servers, AUM network, Computers and the internet access. Besides all AUM sites and remote learning are fully secured. Also, all the servers and PCs have antivirus systems to protect them. In addition, we have Office 365 mail and office solution that is fully secured by Microsoft company which also provides One Drive where the students, Faculties and the Staff will be able to secure their files and documents on it and it gives the ability to share their documents in a very secured manner. In addition, all the AUM systems are secured with a very restrictive access permissions where the access permissions is given as per the business needs after getting a proper approvals. And surly all the personal information data for Students, Staff and

Faculties are fully secured against anonymous access and no one can access it without a proper access permission. All the information data for the students will be placed on the students information system OIS, where no one can see the data of others and no one will have an access without a proper permission

Retention policy

1.Scope

This Policy is aimed at regulating the retention, maintenance and disposal of documentation, both personal and other, within the American University of Malta, and in accordance with the principles of data protection legislation, and other legal provisions in Maltese Law.

2.Background

The GDPR puts forward the principle that personal data and sensitive personal data should not be retained for periods that are longer than necessary. In this context, the American University of Malta will be putting forward a retention policy for all data and documentation that it collects and processes, with the purpose of ensuring compliance to the Regulation and to ensure that no resources are utilized in the processing and archiving of data which is no longer of relevance.

3. Objectives

This policy aims to achieve the following objectives:

a. Regulate the retention of and disposal of the various types of documentation whether held in manual or automated filing systems within the American University of Malta while adhering to the Data Protection principle that personal data should not be retained for a longer period than necessary.
b. Dispose of unnecessary documentation that is no longer relevant and is taking up useful storage space.
c. Promote the digitization of documentation as may be reasonably possible to minimize the use of storage space required to store documentation, as well as to promote sustainable use of paper and printing consumables.

4.Adminstration

Documentation is held in the Aum Network shared folder and each department has separate storage. This Policy is therefore applicable to all such documentation. It will be the responsibility of the relevant Departments, to ensure that all provisions of this Policy are adhered to.

5.Documentation Held within the office of the public service commision

As part of its operating requirements the AUM requests, keeps and maintains a wide range of documentation including personal data. The various types of documentation utilized by American University of Malta may be categorized as follows:

- Personal Data & files of the Students, Faculty and staff.
- Attendance and absence records of students, Faculty.
- Financial records including payrolls and national insurance contributions, etc.
- Administrative and Policy Files.
- Lectures audio-recordings.
-

6. Security of Documentation

Documentation is maintained in an accessible but secure location with adequate access provided to officials who have the clearance level to access the relevant documentation. In the case of documents with sensitive personal data with higher clearance levels, access control protocols are fully adhered, to ensure that only those that have the required security clearance have access to such documentation.

- In the case of personal data, the GDPR also stipulates that only those required to process personal data should have access to personal records.
- Personnel who are found to be in breach of these security protocols, and thus in breach of the GDPR, will be subject to disciplinary action.

7. Retention period

Retention of different categories of documents is governed by different requirements and different legislation and regulations.

IT Risk Management Policy

1.Purpose

To establish a process to manage risks to the University of AUM that result from threats to the confidentiality, integrity and availability of University Data and Information Systems.

2.Scope

This policy applies to all electronic data created, stored, processed or transmitted by the American University of Malta, and the Information Systems used with that data.

3.principles of Data risks

This policy helps to protect AUM from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

4.Policy

- All Information Systems must be assessed for risk to the AUM that results from threats to the integrity, availability and confidentiality of AUM Data. Assessments should be completed prior to purchase of, or significant changes to, an Information System; and at least every 2 years for systems that store, process or transmit Restricted Data.
- Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.
- Residual risks may only be accepted on behalf of the university by a person with the appropriate level of authority as determined by the Information Technology Department. Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated.
- Each Information System must have a system security plan, prepared using input from risk, security and vulnerability assessments.

5.Responsibilities

1. Information Technology Department are responsible for ensuring that their unit conducts risk assessments on Information Systems and uses the university approved process.
2. Information Technology Department and Management is responsible for assessing and mitigating risks using the university approved process.