MIE GDPR Policy

1. Introduction

MIE is committed to protecting the personal data of all students, staff, faculty, and stakeholders in compliance with the **General Data Protection Regulation (GDPR) (EU) 2016/679** and the **Maltese Data Protection Act (Chapter 586)**. This policy outlines the principles of data protection, responsibilities, and procedures to ensure the confidentiality, integrity, and security of personal data.

2. Scope

This policy applies to all staff, faculty, students, contractors, and third-party service providers who handle personal data on behalf of Malta ICOM Educational. It covers all personal data collected, stored, processed, or transferred, whether in physical or digital form, within or outside the European Union (EU).

3. Key Principles

In compliance with the GDPR, MIE ensures that personal data is:

- **Lawfully, fairly, and transparently processed** (Article 5(1)(a))
- **Collected for specified, explicit, and legitimate purposes** (Article 5(1)(b))
- **Adequate, relevant, and limited to what is necessary** (Article 5(1)(c))
- **Accurate and kept up to date** (Article 5(1)(d))
- **Retained for no longer than is necessary** (Article 5(1)(e))
- **Securely processed** with appropriate technical and organizational measures (Article 5(1)(f))

4. Lawful Basis for Processing

In accordance with **Article 6 of the GDPR**, the institution will only process personal data when:

- It is necessary for the performance of a contract (e.g., student enrolment, employment contracts)
- It is necessary to comply with legal obligations (e.g., academic records, tax obligations)
- Explicit consent has been obtained (e.g., marketing communications, sensitive data processing)
- It is in the legitimate interest of MIE (e.g., improving services, alumni relations)

- It is necessary to protect the vital interests of data subjects or other persons

5. Special Categories of Data

In line with **Article 9 GDPR**, special categories of personal data (e.g., health data, biometric data) will only be processed with explicit consent or when required by law. We ensure the highest level of protection for this data through encryption, restricted access, and regular audits.

6. Data Subject Rights

MIE guarantees the rights of data subjects under the GDPR, including:

- **Right to Access** (Article 15): Individuals can request access to their personal data and receive detailed information about how their data is processed.
- **Right to Rectification** (Article 16): Individuals can request corrections to inaccurate or incomplete data.
- **Right to Erasure (Right to be Forgotten)** (Article 17): Individuals can request the deletion of their personal data where it is no longer necessary or if they withdraw their consent.
- **Right to Restriction of Processing** (Article 18): Individuals can request the limitation of data processing under certain conditions.
- **Right to Data Portability** (Article 20): Individuals can receive their personal data in a structured, commonly used format and transfer it to another data controller.
- **Right to Object** (Article 21): Individuals can object to processing activities based on legitimate interests or direct marketing.

Requests should be submitted to the **Data Protection Officer (DPO)** (see contact details below), and we will respond within one month of the request.

7. Data Protection Officer (DPO) Responsibilities

Our **Data Protection Officer (DPO)** is responsible for overseeing data protection activities, advising on GDPR compliance, and acting as the point of contact for data subjects and supervisory authorities.

DPO Responsibilities include:

- Conducting Data Protection Impact Assessments (DPIAs) (Article 35)
- Advising on the processing of personal data and compliance with data protection laws
- Managing data subject requests and complaints

- Conducting audits and ensuring compliance with GDPR guidelines
- Liaising with the Maltese Information and Data Protection Commissioner (IDPC)

Contact Information for DPO: Email: dpo@icomedicine.com

8. Data Security

MIE has implemented appropriate technical and organizational measures to protect personal data in accordance with **Article 32 GDPR**:

- **Access Controls**: Role-based access controls (RBAC) to limit access to personal data to authorized personnel only.
- **Encryption**: All sensitive data is encrypted in transit and at rest.
- **Multi-factor Authentication (MFA)**: For access to sensitive data and systems.
- **Data Breach Notification**: In the event of a data breach, the DPO will notify the Maltese Information and Data Protection Commissioner within 72 hours and affected individuals where required (Article 33).

9. Third-Party Contractors and Data Transfers

In compliance with **Articles 28 and 44-49 GDPR**, MIE ensures that any third-party contractors handling personal data on our behalf are contractually obligated to follow strict data protection measures. Data transfers outside the EU will only be made if appropriate safeguards are in place (e.g., Standard Contractual Clauses).

Third-Party Agreements Must Include:

- Data security requirements
- Confidentiality agreements
- Details of how personal data will be managed and secured
- Procedures for handling data breaches

10. Data Retention and Deletion

Personal data will be retained only for as long as necessary to fulfil the purposes for which it was collected, in compliance with **Article 5(1)(e) GDPR**.

- **Retention Periods**: We have defined specific retention periods for different categories of personal data (e.g., academic records, financial data).
- **Data Deletion**: At the end of the retention period, data will be securely deleted, ensuring that no personal data remains accessible.

11. Monitoring and Audits

Regular audits will be conducted to ensure GDPR compliance. This includes reviewing data access logs, conducting risk assessments, and monitoring third-party contractors. The **DPO** will oversee the implementation of any necessary corrective actions.

12. Data Protection Impact Assessments (DPIAs)

In line with **Article 35 GDPR**, DPIAs will be conducted for any high-risk data processing activities (e.g., new online learning platforms, large-scale processing of health data). The **DPO** will lead the assessment, which will include:

- Identifying and assessing risks to data subjects
- Implementing measures to mitigate risks
- Ensuring full compliance with GDPR

13. Training and Awareness

All employees of Malta ICOM Educational, especially those handling personal data, will receive regular training on data protection principles and GDPR compliance. This will include:

- How to handle data subject requests
- Best practices for secure data handling
- Responsibilities under the GDPR and Maltese Data Protection Act

14. Data Breaches

In the event of a personal data breach, our **DPO** will notify the Maltese **Information and Data Protection Commissioner (IDPC)** within **72 hours** and inform affected individuals where applicable, in compliance with **Article 33 GDPR**.

---

15. Complaints and Contact Information

If any individual has concerns about how their personal data is being processed, they can contact our **Data Protection Officer (DPO)**. Complaints can also be directed to the **Maltese Information and Data Protection Commissioner (IDPC)**.

Contact Information for DPO - Email: dpo@icomedicine.com

16. GDPR Compliance Forms

145. GDPR Compliance Agreement for Third-Party Service Providers/External Contractors

GDPR Policy

144. GDPR Compliance Acknowledgment Form inhouse

These forms will be used during staff induction, contractor agreements, or for students who have access to personal data. All third-party service providers or external contractors will sign similar agreements to ensure they are aligned with your institution's data protection standards.

Accountability: Ensures staff, contractors, or students acknowledge their responsibility in handling personal data.

Evidence of Compliance: Provides a formal record that the institution can show during audits or reviews by regulatory bodies.

Training and Awareness: Ensures that all individuals who interact with personal data are aware of their obligations under GDPR.