# **Fawzooz AI - Data Governance Policy for AI**

Version: 1.0

Effective Date: [Date]

Policy Owner: [e.g., Data Protection Officer (DPO) / Chief Data Officer]

Approved By: [e.g., AI Governance Committee (AIGC)]

### 1. Purpose and Scope

The purpose of this policy is to establish a formal framework for the governance of all data used in the lifecycle of Fawzooz AI's Artificial Intelligence (AI) systems. This policy ensures that data is managed as a critical asset in a manner that is secure, ethical, private, and compliant with all legal and regulatory obligations, including but not limited to GDPR and HIPAA.

Effective data governance is fundamental to our mission of providing safe and trustworthy AI-powered mental wellness applications. It is the foundation upon which the quality, fairness, and security of our AI systems are built.

This policy applies to all Fawzooz AI employees, contractors, and third parties who handle data associated with our AI systems. It covers all data, including personal data, sensitive personal data, and non-personal data, throughout its entire lifecycle—from collection to disposal.

### 2. Core Data Governance Principles

Fawzooz AI commits to the following principles for all data governed under this policy:

* **Lawfulness, Fairness, and Transparency:** Data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
* **Purpose Limitation:** Data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
* **Data Minimization:** We will collect and process only the data that is adequate, relevant, and strictly necessary for the intended purpose.
* **Accuracy:** We will take every reasonable step to ensure that data is accurate and, where necessary, kept up to date.
* **Storage Limitation:** Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
* **Integrity and Confidentiality (Security):** Data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
* **Accountability:** Fawzooz AI is responsible for, and must be able to demonstrate, compliance with these principles.

### 3. Roles and Responsibilities

| **Role** | **Responsibilities** |
| --- | --- |
| **Data Protection Officer (DPO)** | Owns this policy. Provides independent oversight of data protection compliance, acts as the primary contact for regulatory authorities, and advises the organization on all data protection matters. |
| **AI Governance Committee (AIGC)** | Provides strategic oversight for data governance as it relates to AI, ensuring alignment with organizational objectives and risk appetite. |
| **Data Stewards** | Individuals assigned responsibility for specific data domains (e.g., user therapy session data). They are responsible for defining and controlling data quality, access, and usage rules for their domain. |
| **Data Custodians (IT/Engineering)** | Responsible for the technical implementation and management of data storage, security, and access controls as defined by Data Stewards and this policy. |
| **All Personnel** | Responsible for handling data in accordance with this policy and reporting any potential data breaches or policy violations. |

### 4. Data Lifecycle Management

#### 4.1. Data Collection & Sourcing

* **Consent:** Where required, valid, informed consent must be obtained from data subjects before or at the time of data collection. Consent language must be clear, specific, and easily understandable.
* **Third-Party Data:** All third-party data sources must be vetted for legality, quality, and ethical sourcing before acquisition.

#### 4.2. Data Processing & Use

* **Authorized Use:** Data shall only be used for the specific purposes for which it was collected and for which authorization has been granted.
* **De-identification:** Personal data must be pseudonymized or anonymized wherever possible, especially when used for analytics or model training.

#### 4.3. Data Quality for AI

* **Quality Assessment:** All datasets intended for training, validation, or testing of AI models must undergo a formal Data Quality Assessment.
* **Bias Assessment:** Datasets must be rigorously assessed for potential biases (e.g., demographic, cultural, socioeconomic). The results of this assessment and any mitigation steps taken must be documented.
* **Data Provenance:** A complete record of data provenance (origin, lineage, and transformations) must be maintained for all AI training datasets to ensure traceability and reproducibility.

#### 4.4. Data Storage, Security, and Access

* **Data Classification:** All data must be classified according to the Fawzooz AI Data Classification Scheme (e.g., Public, Internal, Confidential, Restricted).
* **Access Control:** Access to data is granted on a strict "need-to-know" basis, following the principle of least privilege. Access to "Restricted" data (e.g., sensitive mental health information) requires explicit approval from the designated Data Steward and the DPO.
* **Encryption:** All sensitive data must be encrypted both at rest and in transit.

#### 4.5. Data Retention and Disposal

* **Retention Schedule:** Data will be retained only as long as necessary to fulfill its intended purpose or as required by law. A formal Data Retention Schedule will be maintained.
* **Secure Disposal:** When data is no longer needed, it must be disposed of securely using methods that ensure it is irrecoverable.

### 5. Policy Compliance and Auditing

* Compliance with this policy is mandatory.
* The DPO will oversee regular audits and monitoring to ensure adherence to this policy.
* Any suspected or actual data breach must be immediately reported to the DPO in accordance with the Data Breach Incident Response Plan.
* Violations of this policy will be subject to disciplinary action.

**End of Policy**