# **AI Ethics & Legal Compliance Policy – [Nome Progetto/Organizzazione]**

**Data:** [gg/mm/aaaa]

**Versione:** [v1.0]

**Responsabile:** [Nome, Ruolo]

## **1. Scopo e ambito**

Definire i principi etici e le regole di conformità legale nell’uso, sviluppo e manutenzione di sistemi di Intelligenza Artificiale.

## **2. Principi etici fondamentali**

* **Trasparenza:** Chiarezza su funzionamento, scopi e limiti dei sistemi AI.
* **Non discriminazione:** Impegno concreto a evitare bias e garantire equità.
* **Responsabilità:** Assegnazione chiara di responsabilità per sviluppo, gestione, supervisione e intervento.
* **Sicurezza:** Tutela dati e prevenzione di rischi informatici o di danno fisico/morale.
* **Rispetto della dignità umana e dei diritti fondamentali:** Inclusi privacy, libertà di scelta e informazione.

## **3. Conformità legale**

* **Riferimenti normativi:**
  + EU AI Act
  + ISO 42001
  + GDPR
  + DDL 1433 (Italia, in corso di approvazione)
  + Altri regolamenti settoriali applicabili
* **Obblighi chiave:**
  + Valutazione rischio e impatti
  + Documentazione di processi, dati, logiche decisionali
  + Supervisione umana e tracciabilità interventi
  + Auditabilità e possibilità di revisione/contestazione

## **4. Implementazione nel ciclo di vita del sistema AI**

* **Progettazione:**
  + Analisi etica ex ante, inclusa valutazione rischi sociali e di bias
  + Coinvolgimento stakeholder rilevanti
* **Sviluppo:**
  + Applicazione di linee guida tecniche per privacy, fairness, sicurezza
  + Adozione di metriche e audit periodici
* **Deployment e uso:**
  + Supervisione umana sempre prevista su output critici
  + Logging e trasparenza verso utenti/interessati
  + Gestione efficace di segnalazioni e reclami
* **Aggiornamento e miglioramento:**
  + Monitoraggio costante, formazione, revisione policy ad ogni cambio normativo o tecnico rilevante

## **5. Ruoli e responsabilità**

| **Ruolo** | **Compiti principali** |
| --- | --- |
| AI Responsible Officer | Coordinamento compliance, formazione, revisione |
| Data Protection Officer | Privacy, minimizzazione e anonimizzazione dati |
| IT Security Manager | Sicurezza infrastruttura e modelli |
| Human Oversight Team | Supervisione, escalation, gestione incidenti |
| Utenti finali e stakeholder | Segnalazione rischi, richieste di informazione |

## **6. Audit e miglioramento continuo**

* **Audit periodici** su rischi etici e legali (almeno annuale)
* Aggiornamento policy in base a nuovi rischi, normative, best practice
* Report pubblico (o interno) di conformità

## **7. Comunicazione e formazione**

* Informazione chiara a utenti, clienti, dipendenti sull’uso dell’AI
* Formazione periodica di tutto il personale coinvolto

## **8. Gestione segnalazioni e incidenti**

* Canale dedicato per segnalazioni di rischi, bias, errori, incidenti
* Procedura rapida di presa in carico, analisi e risposta
* Log di tutte le segnalazioni gestite

## **9. Allegati**

* Policy privacy e data protection
* Report di audit etico e legale
* Procedure di intervento e supervisione

**[Firma, data, eventuale timbro]**