AI Governance e Compliance: Semplificare e centralizzare io governo dell'AI

Claudio Stamile, PhD, MBA – Manager of AI R&D @ Fastweb+Vodafone

La compliance di un singolo use-case AI è complessa, multidimensionale e costosa. Serve metodo, competenze e governance economica.

AI ACT – RISK LEVEL

Classificazione, requisiti e obblighi specifici

RISCHIO INACCETTABILE	**Divieto di utilizzo** Sistemi manipolativi, social scoring, ecc.
ALTO RISCHIO	**Obblighi stringenti** Gestione rischio, qualità dati, trasparenza, documentazione tecnica, human oversight, robustezza, audit, registrazione EU database
RISCHIO LIMITATO	**Obblighi di trasparenza** Informare l'utente che sta interagendo con un sistema AI
RISCHIO MINIMO	**Nessun obbligo specifico** Buone pratiche raccomandate

GDPR – PROTEZIONE DEI DATI PERSONALI

Principi e adempimenti applicabili

- **BASE GIURIDICA DEL TRATTAMENTO**
  Definizione e documentazione della liceità del trattamento
- **DATA MINIMIZATION**
  Raccolta e utilizzo dei soli dati necessari
- **DIRITTI DELL'INTERESSATO**
  Accesso, rettifica, cancellazione, opposizione, portabilità
- **DPIA (VALUTAZIONE D'IMPATTO)**
  Obbligatoria per trattamenti ad alto rischio
- **SICUREZZA E DATA GOVERNANCE**
  Misure tecniche e organizzative adeguate
- **RESPONSABILITÀ E ACCOUNTABILITY**
  Registro dei trattamenti, nomine, accordi con responsabili

COPYRIGHT E DIRITTI CONNESSI

Utilizzo lecito dei contenuti e dei modelli

- **FONTE DEI DATI DI TRAINING**
  Verifica licenze, termini d'uso e diritti sui dataset
- **DIRITTI SU CONTENUTI GENERATI**
  Valutazione dell'originalità e del rischio di violazione
- **ATTRIBUZIONE E TRASPARENZA**
  Indicazioni di fonte quando richiesto
- **GESTIONE DELLE LICENZE**
  Tracciabilità delle licenze e delle autorizzazioni

FATTORI CHE AUMENTANO LA COMPLESSITÀ

- Eterogeneità dei dati e delle fonti
- Evoluzione continua dei modelli
- Integrazione con sistemi e processi esistenti
- Ambiguità normativa e linee guida in evoluzione
- Molteplici stakeholder coinvolti

GOVERNANCE DEI COSTI DELLA COMPLIANCE AI

1. **ASSESSMENT**
   Analisi del contesto, dei rischi e dei requisiti applicabili
2. **PIANIFICAZIONE**
   Definizione delle attività, delle risorse e delle priorità
3. **ESECUZIONE**
   Implementazione di misure tecniche, organizzative e documentali
4. **MONITORAGGIO**
   Controlli, audit, aggiornamenti e miglioramento continuo

VOCI DI COSTO PRINCIPALI

- Consulenza legale e regolatoria
- Valutazioni di impatto e risk management
- Sviluppo e adeguamento tecnico
- Data governance e qualità dei dati
- Formazione e change management
- Audit e monitoraggio continuo

RISULTATO
Riduzione del rischio normativo e reputazionale, sostenibilità economica e fiducia nel tempo

Ogni use-case AI richiede un percorso di compliance su misura. | Senza una governance strutturata, i costi crescono e i rischi si moltiplicano. | Compliance non è un adempimento: è un investimento in valore, sicurezza e fiducia.

SCALARE L'AI RICHIEDE SCALARE ANCHE GOVERNANCE E COMPLIANCE

Con un'adozione AI pervasiva, la compliance non può diventare un collo di bottiglia operativo.

1. L'ADOZIONE AI NELL'ORGANIZZAZIONE

PRODUTTORI DI DATI	600+
CONSUMATORI DI DATI	1350+
PROFESSIONISTI AI	110+
USE CASE IN PRODUZIONE	104
USE CASE IN PIPELINE	141
DIPENDENTI CHE UTILIZZANO AI	72%

2. PERCHÉ LA COMPLESSITÀ CRESCE

PIÙ USE CASE

↓

PIÙ OBBLIGHI

- AI Act
- GDPR
- Copyright
- Security
- Cost Governance

↓

PIÙ ATTIVITÀ DI COMPLIANCE

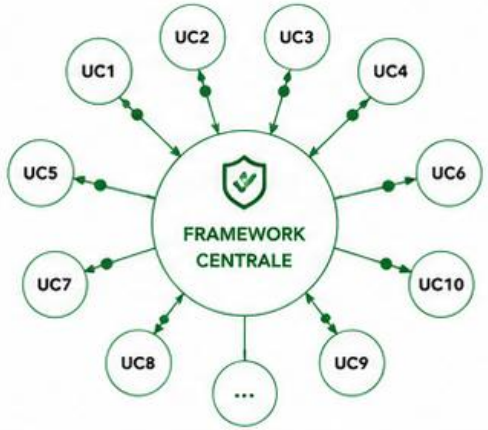
- Assessment
- Documentazione
- Audit
- Monitoraggio
- Aggiornamento continuo

3. DUE APPROCCI A CONFRONTO

MODELLO CENTRALIZZATO

Tutti gli use case convergono verso un unico team centrale creando collo di bottiglia, ritardi e costi elevati.

MODELLO HUB & SPOKE ABILITATO

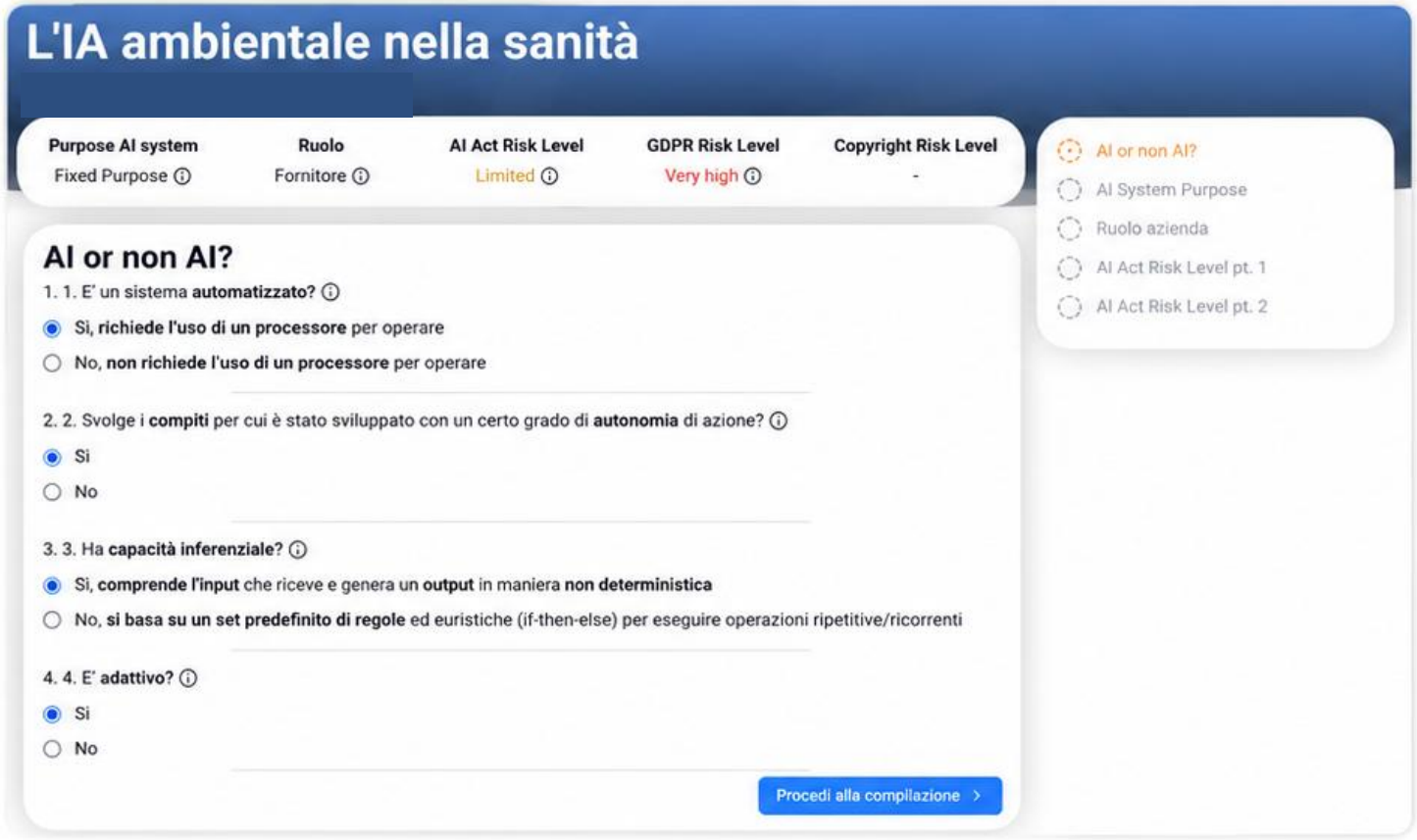


Compilazione distribuita degli use case con governance centrale, controlli automatici e piena tracciabilità.

L'OBIETTIVO NON È CENTRALIZZARE LA COMPLIANCE.
L'OBIETTIVO È DEMOCRATIZZARE LA COMPLIANCE MANTENENDO IL CONTROLLO.
Framework centrale + spoke autonomi = AI scalabile, conforme e sostenibile.

VALUTARE IL SISTEMA PER CLASSIFICARE IL RISCHIO AI ACT

Un questionario guidato trasforma le caratteristiche tecniche del sistema in una valutazione chiara del rischio normativo e degli obblighi applicabili.



1. QUESTIONARIO GUIDATO

Domande semplici e mirate per identificare le caratteristiche chiave del sistema.

2. VALUTAZIONE AUTOMATICA

Il sistema determina il livello di rischio AI Act, GDPR e Copyright.

3. CLASSIFICAZIONE CHIARA

Output immediato del risk level e degli obblighi applicabili.

4. PERCORSO STRUTTURATO

Navigazione step-by-step per completare la classificazione del sistema.

Una classificazione corretta è il primo passo per una governance efficace, conforme e basata su evidenze.

ANALIZZARE IL SISTEMA PER DEFINIRE SCOPO E CONTESTO D'USO

Raccolta strutturata delle informazioni chiave per comprendere il sistema AI e valutare impatto, rischi e ambito normativo.

AI System Purpose

6. 6. Descrizione progetto:

Il sistema AI ascolta, registra, trascrive le conversazioni medico-paziente; riassume e struttura la conversazione stessa; codifica le informazioni amministrative (es: codice patologia ecc.). Supporta il medico offrendo una bozza del referto che il medico deve validare.

7. 7. Il sistema di AI può **svolgere** con competenza **un'ampia gamma di compiti distinti** in più contesti?

- ○ Sì, può essere applicato in maniera ampia e trasversale per svolgere **una serie di compiti distinti in più contesti**
- ◉ No, **è addestrato per eseguire compiti specifici e operare all'interno di un ambiente predefinito.**

11. 11. Il sistema di AI è un **chatbot**?

- ○ Sì, **l'interazione** con l'utente può riguardare **qualsiasi argomento**
- ○ Sì, **l'interazione** con l'utente riguarda **esclusivamente argomenti predefiniti** e limitati
- ◉ **No**

12. 12. Per il funzionamento del sistema di AI viene integrato un **modello di AI per finalità generali** (LLM)?

- ◉ Sì
- ○ No

13. 13. **Qual è?** Indicare modello generale di AI per finalità generali integrato all'interno del sistema di AI.

Azure

16. 16. L'integrazione del modello di AI per finalità generali all'interno del sistema di AI è **limitata al perseguimento di uno scopo ben definito?**

- ◉ **Sì, il modello generale è limitato** per consentire al sistema di AI di svolgere esclusivamente compiti specifici **all'interno di un contesto predefinito**
- ○ No, l'integrazione con il modello generale **consente al sistema di AI di svolgere una serie di compiti distinti in contesti molteplici**

1. DESCRIZIONE DEL SISTEMA

Definizione chiara dello scopo e delle funzionalità principali del sistema AI.

2. CONTESTO D'USO

Analisi dell'ambito operativo e della varietà dei compiti svolti dal sistema.

3. MODALITÀ DI INTERAZIONE

Valutazione del tipo di interazione e dei limiti di utilizzo per l'utente.

4. INTEGRAZIONE DI MODELLI GENERALI

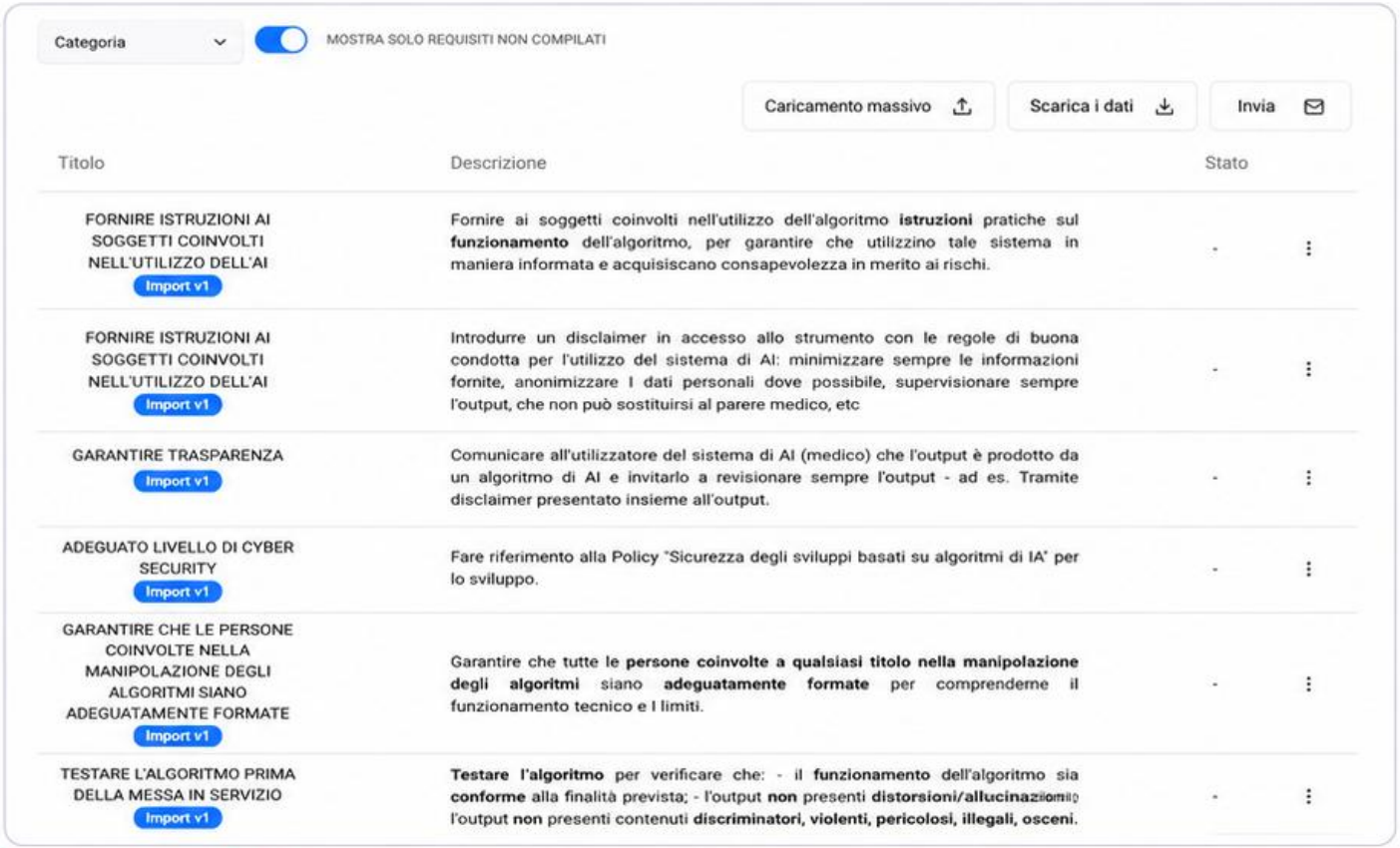
Verifica dell'uso di LLM o modelli general purpose e del loro perimetro di impiego.

5. PERIMETRO OPERATIVO

Definizione del grado di limitazione del modello rispetto a scopi e contesti specifici.

I REQUISITI DI COMPLIANCE: GLI OBBLIGHI DA SODDISFARE E TRACCIARE

Il sistema genera l'elenco dei requisiti applicabili al progetto AI in base al rischio e al contesto d'uso.
Ogni requisito è da implementare e tracciare con evidenze oggettive per garantire compliance e accountability.



OUTPUT DEL PROCESSO DI GOVERNANCE

ELENCO REQUISITI APPLICABILI
- Determinati in base a rischio, categoria AI Act e contesto d'uso

DETTAGLIO DEL REQUISITO
- Descrizione chiara dell'obbligo da soddisfare
- Indicazioni operative e riferimenti normativi

TRACCIABILITÀ EVIDENZE
- Stato di avanzamento e completamento
- Raccolta e conservazione delle evidenze a supporto

ACCOUNTABILITY E CONTROLLO
- Tracciabilità per audit interni ed esterni
- Dimostrazione di conformità e accountability verso gli stakeholder

OGNI REQUISITO È UN IMPEGNO DA SODDISFARE E DOCUMENTARE.
SENZA EVIDENZE NON C'È COMPLIANCE. SENZA TRACCIABILITÀ NON C'È CONTROLLO.

Grazie

Claudio Stamile, PhD, MBA – Manager of AI R&D @ Fastweb+Vodafone