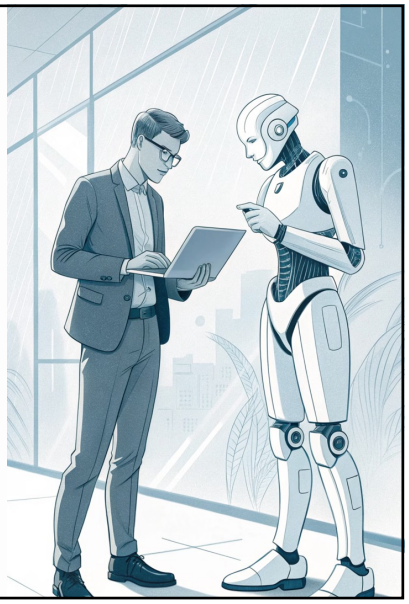
INTELLIGENZA ARTIFICIALE: ETICA E DEONTOLOGIA PROFESSIONALE

a cura di

Ing.Francesco Marinuzzi, Ph.D.

Prompt Engineer

www.marinuzzi.it



1

Quadro Normativo Italiano: Etica e Deontologia nell'AI

In Italia, l'etica e la deontologia dell'IA sono regolate dal Regolamento UE AI Act (2024/1689) e integrate dalla Legge n. 132/2025. Tali normative impongono un approccio antropocentrico, sottolineando trasparenza, responsabilità umana e non discriminazione.

AI Act e Rischio

Classifica i sistemi AI per rischio, con obblighi stringenti per quelli ad alto rischio, richiedendo valutazioni di conformità.

Legge 132/2025

Introduce obblighi nazionali come l'informativa al cliente sull'uso di AI e la tracciabilità degli algoritmi.

Principi Etici

Antropocentrismo, trasparenza, protezione dati e divieto di bias discriminatori sono al centro.

Applicazioni Deontologiche

Per i professionisti, impone verifica umana degli output e obbligo di informare il cliente (es. settore legale).

2

Etica e Deontologia degli Ingegneri Italiani

Il Codice Deontologico del Consiglio Nazionale Ingegneri (CNI), approvato il 14 giugno 2023 (delibera n. 88/2023), stabilisce i principi etici e professionali. È aggiornato per l'equo compenso (L. 49/2023) e le modifiche costituzionali (artt. 9 e 41), guidando la condotta degli ingegneri italiani.

Struttura Fondamentale

Comprende 23 articoli su integrità, autonomia, diligenza e riservatezza. Definisce doveri verso clienti ed enti pubblici, includendo sanzioni per violazioni fiscali e compensi non equi.

Novità Chiave 2023

Introduce l'obbligo di compensi equi (art. 10-11), rafforza l'autonomia intellettuale da pressioni (art. 3.4) e vieta critiche denigratorie tra colleghi (art. 13). Recepito dagli Ordini provinciali.

3

Riferimenti Documentali

Accedi facilmente ai testi integrali delle normative e dei codici etici menzionati tramite i QR code sottostanti.

Regolamento UE AI Act

Regolamento (UE) 2024/1689 sull'intelligenza artificiale.113 articoli, 13 Allegati, 144pp

Legge n. 132/2025

Norme italiane sull'applicazione dell'IA e requisiti aggiuntivi. 28 articoli

Codice Deontologico CNI

Consiglio Nazionale Ingegneri, delibera n. 88/2023. 23 articoli 17 pp.

4

Il Prompting: il nuovo Codice dei Sistemi Digitali

Il prompting rappresenta il nuovo linguaggio che trasforma l'intelligenza artificiale in strumenti specializzati, creando valore digitale in modo più intuitivo e potente.

Il vecchio codice

Linguaggi di programmazione strutturavano sistemi specializzati attraverso sintassi rigide e regole precise.

- Richiede conoscenze tecniche avanzate
- Modifiche complesse e time-consuming
- Limitato a sviluppatori professionisti

Il nuovo codice

Il prompting guida le intelligenze artificiali con istruzioni in linguaggio naturale e design accurato.

- Flessibilità e adattamento rapido
- Accessibilità per utenti non tecnici
- Integrazione con basi documentali esistenti

La trasformazione

Come il software ha specializzato i computer generici, il prompting insieme ai modelli LLM riscrive l'interazione con sistemi digitali.

- **Nuovo asset immateriale strategico**
- Democratizzazione dell'accesso all'AI
- Evoluzione continua e personalizzabile

5

Gli Agenti AI: Il nuovo Asset immateriale

Basati su robuste basi documentali e un innovativo sistema di prompting, gli Agenti AI stanno rivoluzionando il valore immateriale nel digitale.

Agenti AI

Il nuovo valore digitale

Sistema di prompting su LLM

Istruzioni strategiche e specifiche

Basi documentali

Fondamenta robuste e strutturate

Questa nuova classe di asset immateriali rappresenta un cambio di paradigma nella creazione di valore nell'era digitale, spostando il focus dalle competenze di programmazione tradizionale alla capacità di formulare istruzioni efficaci (prompting).

6

Ecosistema di Agenti AI Interconnessi

Gli Agenti AI possono esser progettati per costituire reti collaborative di intelligenza in comunicazione tra loro e anche con gli utenti umani.

Agenti Specializzati

Ogni agente possiede competenze, carattere, specifiche e collabora con altri per risolvere problemi complessi.

Interazione Umana

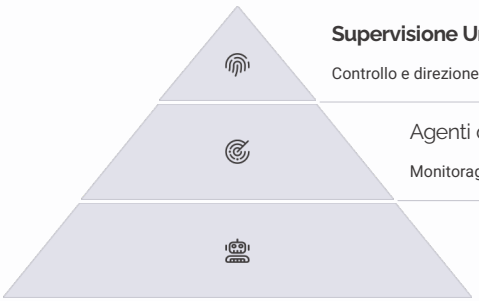
L'interfaccia naturale permette una comunicazione fluida tra persone e agenti, creando partnership produttive.

Rete Cooperativa

L'interconnessione tra agenti moltiplica le capacità del sistema generando soluzioni innovative.

7

Controllo a Torre: Agenti di Controllo per un Sistema Monitorato dall'Uomo



Supervisione Umana

Controllo e direzione strategica

Agenti di Controllo - **Agente ETICO**

Monitoraggio e coordinamento del sistema

Agenti AI Operativi

Esecuzione di compiti specifici

Questa struttura gerarchica garantisce che gli agenti AI operino all'interno di un framework controllato, dove **l'intelligenza artificiale aumenta le capacità umane mantenendo l'uomo al centro del processo decisionale.**

8

Un Agente AI Esperto: ***Ing. EtAI***

Un innovativo Agente AI specializzato in etica e deontologia, progettato per supportare gli ingegneri italiani nell'applicazione delle normative sull'intelligenza artificiale e dei principi professionali.

Domande e Risposte

Risponde puntuale a dubbi sulla normativa vigente e sulla sua interpretazione.

Adempimenti

Vi supporta nella stesura e nella messa in "atto" e nella governance degli adempimenti previsti dalla normativa..

Dilemmi

Assiste nella valutazione e risoluzione di dilemmi etici legati alla attività professionale e all'uso dell'AI.

9

L'Agente AI Etico: **Ing. EtAI**

Scansiona per Accedere

Utilizza il tuo smartphone per interagire direttamente con il nostro Agente AI Etico, un supporto intelligente per le tue esigenze normative e deontologiche.

Dietro le Quinte: Il Processo di Creazione

Lo sviluppo dell'Agente AI Etico ha coinvolto una **rigorosa selezione** e integrazione di testi normativi vigenti e del codice deontologico degli ingegneri italiani . Questo include il Regolamento UE AI Act il Codice Deontologico CNI e la legge italiana 132/2025.

Il modello è stato poi **addestrato e ottimizzato** su questi specifici documenti, garantendo risposte contestualizzate e conformi alle normative più recenti. L'obiettivo è fornire un assistente affidabile per l'interpretazione e l'applicazione delle direttive etiche e professionali nel campo dell'IA dedicato ai colleghi ingegneri che li aiuti anche a semplificare i tanti adempimenti previsti.

Attualmente (2026) esiste in due versioni. Uno liberamente accessibile nel mercato dei GPT di OpenAI all'indirizzo del QRcode e l'altro in ambiente "Custom" Oystar con LLM locali e integrabile con altri agenti via protocolli fra agenti e/o API tale da garantire massima privacy e riservatezza. Per la seconda versione contattare l'Ing. Marinuzzi ai riferimenti del sito https://www.marinuzzi.it

LINK

https://chatgpt.com/g/g-697d1ee42f3c8191bc7e4e29ae71cda8-ing-etai

10

Sessione di prova dell'agente

11

Esempi:cosa dice l'articolo 92 dell'AI ACT EU?

- Richiamo secco – Articolo 92 AI Act (Reg. UE 2024/1689)

1. Testo (estratto fedele) Articolo 92 — Potere di effettuare valutazioni Comma 1 – [[Reg2024-1689 Art.92 c.1]] L'Ufficio per l'IA, previa consultazione del Consiglio per l'IA, può effettuare valutazioni sui modelli di IA per finalità generali: a) per verificare la conformità del fornitore agli obblighi del Regolamento quando le informazioni raccolte ai sensi dell'art. 91 sono insufficienti; b) per indagare sui rischi sistemici a livello UE dei modelli di IA per finalità generali con rischio sistemico, anche a seguito di segnalazioni qualificate del gruppo di esperti scientifici. Comma 2 – [[Reg2024-1689 Art.92 c.2]] La Commissione può nominare esperti indipendenti per effettuare le valutazioni per suo conto. Comma 3 – [[Reg2024-1689 Art.92 c.3]] Ai fini delle valutazioni, la Commissione può richiedere accesso al modello (API, altri mezzi tecnici), incluso il codice sorgente. Comma 4 – [[Reg2024-1689 Art.92 c.4]] La richiesta di accesso deve indicare base giuridica, scopo, motivi, termini e le sanzioni pecuniarie applicabili in caso di mancata collaborazione. Comma 5 – [[Reg2024-1689 Art.92 c.5]] I fornitori (o i loro rappresentanti legali) devono fornire l'accesso e le informazioni richieste. Comma 6 – [[Reg2024-1689 Art.92 c.6]] La Commissione adotta atti di esecuzione per definire modalità e condizioni delle valutazioni e il coinvolgimento degli esperti indipendenti. Comma 7 – [[Reg2024-1689 Art.92 c.7]] Prima di richiedere l'accesso, l'Ufficio per l'IA può avviare un dialogo strutturato con il fornitore per approfondire prove interne, garanzie e misure di mitigazione dei rischi sistemici.
2. Quanti commi ha? 👉 L'articolo 92 ha 7 commi.
3. Implicazione pratica (2 righe) Se sei fornitore di modelli di IA per finalità generali (specie con rischio sistemico), devi essere

12

Esempi: Per il mio studio professionale se uso Chat GPT per controllare i progetti e fare alcuni documenti che devo fare per essere compliance?

- Se usi ChatGPT come supporto interno (controllo, revisione, bozze): sei deployer di un sistema AI a basso rischio, non devi certificare nulla, devi però: governare l'uso, evitare deleghe decisionali, tutelare dati/cliente e documentare il controllo umano.

1. Inquadramento (contesto + assunzioni) Assumo che: lo studio non vende AI (non sei provider), usi ChatGPT per: controllo formale/tecnico dei progetti, redazione o revisione di relazioni, capitolati, documenti tecnici, l'output viene sempre validato da un professionista. ➡️ In questo caso sei deployer di AI generativa per uso professionale interno.
2. Riferimenti normativi (ancore rilevanti) AI Act – Reg. (UE) 2024/1689 [[Reg2024-1689 Art.3]] – definizioni (sistema AI, deployer) [[Reg2024-1689 Art.4]] – obbligo di alfabetizzazione AI [[Reg2024-1689 Art.50 c.1]] – trasparenza (quando rilevante) [[Reg2024-1689 Rec.60]] – uso professionale di AI generativa Codice Deontologico CNI [[CNI 4.1]] – responsabilità personale dell'ingegnere [[CNI 5.1]] – correttezza e non inganno [[CNI 6.1]] – competenza e controllo delle tecnologie [[CNI 6.2]] – responsabilità sugli effetti dell'uso tecnologico Legge italiana 132/2025 [[L132 Art.7 c.1]] – diligenza e controllo nell'uso dell'AI [[L132 Art.13]] – professioni intellettuali e AI
3. Interpretazione operativa (cosa significa "nella vita vera") ✓ Cosa è CONSENTITO Usare ChatGPT per: checklist tecniche, verifica coerenza normativa, bozze di testi, supporto al ragionamento. Migliorare produttività e qualità se la decisione finale è tua. ❌ Cosa NON è ammesso (rischioso) Far firmare o consegnare documenti non compresi e verificati. Dire (implicitamente o esplicitamente) che: "il progetto è stato verificato dall'AI" Usare l'AI come sostituto del giudizio professionale (violazione diretta [[CNI 4.1]]).
4. Cosa devi fare per essere compliance (checklist) ✅ OGGI (minimo indispensabile) ☐ Dichiarare internamente che l'AI è strumento di supporto ☐ Stabilire che la responsabilità resta del professionista ☐ Vietare l'inserimento di: dati sensibili dei clienti, documenti riservati non anonimizzati ☐ Verificare che l'output sia sempre revisionato ✅ ENTRO 30 GIORNI ☐ Nota interna / policy AI dello studio scopi ammessi scopi vietati obbligo di revisione umana ☐ Mini-registro d'uso AI tipo attività (bozza, controllo, sintesi) responsabile ☐ Formazione minima (anche 1 ora) sull'uso consapevole → obbligo di AI literacy [[Reg2024-1689 Art.4]] ✅ ENTRO 90 GIORNI (best practice prudente) ☐ Inserire nei modelli di relazione una clausola tipo: "Strumenti di intelligenza artificiale sono stati utilizzati come supporto redazionale; il contenuto è stato integralmente verificato e validato dal professionista." ☐ Procedura di gestione errore AI ☐ Valutazione annuale dei rischi (anche 1 pagina)
5. Evidenze da conservare Policy AI firmata Registro sintetico degli usi Tracce di revisione (commenti, versioni) Attestazione di formazione Template di disclaimer (se usato)
6. Rischi ed errori tipici (quelli che vedo spesso) ❌ "È solo una bozza, non serve controllo" → falso ❌ Copiare output AI senza capirlo ❌ Inserire dati di clienti / gare / CTU ❌ Confondere supporto tecnico con delega decisionale ❌ Nessuna evidenza documentale dell'uso
7. Conclusione netta 👉 Usare ChatGPT è lecito e compatibile con AI Act, Legge 132/2025 e Codice CNI 👉 a condizione che: l'AI non decida, il professionista capisca, controlli e risponda, l'uso sia governato e documentabile. Domanda decisiva (una sola) 👉 I documenti/progetti che fai con supporto AI vengono consegnati a clienti o PA, oppure restano solo uso interno?

13

Segue

- Se consegni al cliente documenti/progetti realizzati con supporto di ChatGPT: puoi farlo legittimamente, devi garantire controllo umano, responsabilità professionale e correttezza informativa, serve una trasparenza "sobria", non allarmistica, documenta l'uso per tutelarti (AI Act + CNI + L.132).

1. Inquadramento (contesto + assunzioni) Assumo che: tu sia studio professionale (ingegnere), usi ChatGPT per bozze, verifiche, riorganizzazione testi, supporto tecnico, il documento finale viene firmato da te ed è usato dal cliente (privato o PA). ➡️ Sei deployer professionale che consegna output a terzi.
2. Riferimenti normativi (ancore rilevanti) AI Act – Reg. (UE) 2024/1689 [[Reg2024-1689 Art.4]] – alfabetizzazione e uso consapevole dell'AI [[Reg2024-1689 Art.50 c.1]] – trasparenza verso le persone interessate [[Reg2024-1689 Rec.60]] – uso professionale di AI generativa come supporto Codice Deontologico CNI [[CNI 4.1]] – responsabilità personale e non delegabile [[CNI 5.1]] – correttezza, lealtà, divieto di inganno [[CNI 6.1]] – controllo degli strumenti tecnologici [[CNI 6.2]] – responsabilità sugli effetti dell'uso Legge italiana 132/2025 [[L132 Art.7 c.1]] – dovere di diligenza e controllo [[L132 Art.13]] – uso dell'AI nelle professioni intellettuali
3. Interpretazione operativa (chiaro e netto) Punto chiave 👉 Non è obbligatorio dire "ho usato ChatGPT" in modo plateale, 👉 ma è obbligatorio non ingannare il cliente e mantenere la piena responsabilità. La norma non ti chiede trasparenza tecnologica totale, ma: trasparenza sul processo, assenza di delega decisionale, tracciabilità e controllo umano.
4. Cosa DEVI fare se consegni al cliente (checklist) ✅ OBBLIGATORIO (oggi) ☐ Responsabilità esplicita il documento è tuo, non dell'AI firmato e validato da te (fondamentale: [[CNI 4.1]]) ☐ Controllo umano sostanziale comprendi contenuti, calcoli, norme citate niente "copia-incolla cieco" ☐ Protezione dati cliente NO dati sensibili / riservati su sistemi AI pubblici anonimizzazione o sintesi se usi l'AI ✅ ENTRO 30 GIORNI (fortemente consigliato) ☐ Clausola standard nei documenti o nel contratto "Nell'ambito dell'attività professionale possono essere utilizzati strumenti digitali avanzati, inclusi sistemi di intelligenza artificiale, esclusivamente come supporto redazionale e di analisi. Il contenuto è stato integralmente verificato e validato dal professionista, che ne assume la piena responsabilità." ☐ Policy AI dello studio (1–2 pagine) cosa è ammesso cosa è vietato obbligo di revisione ☐ Registro minimo d'uso "supporto redazionale / verifica / sintesi" responsabile (non serve dettagliare prompt) ✅ ENTRO 90 GIORNI (best practice difensiva) ☐ Formazione documentata (AI literacy) [[Reg2024-1689 Art.4]] ☐ Procedura "errore AI" ☐ Riesame periodico dei rischi
5. Evidenze da conservare (ti salvano in caso di contestazioni) Policy AI firmata Clausola contrattuale / disclaimer Versioni del documento con note di revisione Registro d'uso Attestazione formazione
6. Errori tipici (⚠️ da evitare assolutamente) ❌ Dire o far intendere che "l'AI ha verificato il progetto" ❌ Consegnare output non compreso ❌ Inserire dati del cliente nei prompt ❌ Nessuna traccia dell'uso dell'AI ❌ Pensare che "tanto lo fanno tutti" (questi sono rischi disciplinari, non solo tecnici)
7. Linea rossa (chiara) 🔴 Non è mai accettabile: delegare valutazioni tecniche o normative all'AI, usare l'AI come "scudo" di responsabilità, ingannare il cliente sul processo professionale.

14

Segue

- Se consegni documenti/progetti a una Pubblica Amministrazione usando ChatGPT come supporto: è lecito, non devi dichiarare il tool, devi dimostrare: controllo umano, responsabilità professionale, tracciabilità del processo e tutela dei dati. Con la PA serve una formalizzazione minima in più rispetto ai clienti privati.

1. Inquadramento (contesto + assunzioni) Assumo che: tu sia studio professionale incaricato dalla PA (affidamento, gara, supporto tecnico), consegni relazioni, progetti, pareri, elaborati tecnici, l'AI sia usata solo come supporto (bozze, controllo, riorganizzazione, sintesi). ➡️ Sei deployer professionale verso soggetto pubblico.
2. Riferimenti normativi (ancore rilevanti) AI Act – Reg. (UE) 2024/1689 [[Reg2024-1689 Art.4]] – alfabetizzazione e uso consapevole dell'AI [[Reg2024-1689 Art.50 c.1]] – trasparenza quando rilevante [[Reg2024-1689 Rec.60]] – AI generativa come supporto professionale Legge italiana 132/2025 [[L132 Art.7 c.1]] – dovere di diligenza e controllo nell'uso dell'AI [[L132 Art.14]] – uso dell'AI nella Pubblica Amministrazione [[L132 Art.13]] – professioni intellettuali Codice Deontologico CNI [[CNI 4.1]] – responsabilità personale e non delegabile [[CNI 5.1]] – correttezza e lealtà verso il committente [[CNI 6.1]] – controllo delle tecnologie [[CNI 6.2]] – responsabilità sugli effetti dell'uso
3. Interpretazione operativa (PA = cosa cambia davvero) Punto fermo 👉 La PA non riceve "output AI" 👉 Riceve un elaborato professionale umano, di cui tu rispondi integralmente. La PA: non ti chiede se usi ChatGPT, ti chiede affidabilità, tracciabilità, controllo e assenza di rischi.
4. Cosa DEVI fare se il cliente è PA (checklist) ✅ OBBLIGATORIO (subito) ☐ Responsabilità esplicita il documento è firmato da te nessun riferimento a "verifica automatica" ([[CNI 4.1]]) ☐ Controllo umano dimostrabile contenuti compresi riferimenti normativi verificati scelte motivate ☐ Tutela dati PA ❌ NO dati riservati, personali, strategici su AI pubbliche se serve supporto AI → astrazione / anonimizzazione ✅ ENTRO 30 GIORNI (fondamentale con PA) ☐ Nota metodologica / clausola tecnica (nel contratto o allegata) "L'attività professionale è svolta mediante strumenti informatici di supporto, inclusi sistemi di intelligenza artificiale, utilizzati esclusivamente come ausilio redazionale e di analisi. Le valutazioni tecniche e le decisioni professionali restano integralmente in capo al professionista incaricato." ☐ Policy AI dello studio ambiti ammessi ambiti vietati obbligo di revisione umana (serve come evidenza ex [[L132 Art.7 c.1]]) ☐ Registro sintetico d'uso AI tipo di supporto responsabile progetto PA coinvolto ✅ ENTRO 90 GIORNI (best practice "anti-contestazione") ☐ Formazione documentata (AI literacy) [[Reg2024-1689 Art.4]] ☐ Procedura di gestione errori ☐ Riesame periodico dei rischi PA
5. Evidenze da conservare (con la PA sono decisive) Contratto / incarico con clausola AI Policy AI dello studio Registro d'uso Versioni dei documenti con revisioni Attestazione formazione 👉 In caso di accesso agli atti / contenzioso, sei coperto.
6. Errori tipici con la PA (⚠️ qui si sbaglia spesso) ❌ Scrivere "verificato con AI" ❌ Inserire dati PA nei prompt ❌ Nessuna traccia del processo ❌ Affidarsi a riferimenti normativi non controllati ❌ Pensare che "la PA non guarda queste cose"
7. Linea rossa (non superabile) 🔴 Mai: delegare valutazioni tecniche/normative all'AI, usare l'AI per decisioni discrezionali, presentare output AI come "neutro" o "oggettivo". Questo sarebbe incompatibile con [[L132 Art.14]] e [[CNI 4.1]].

15

Esempi: voglio sviluppare una soluzione intelligente con vari agenti per un cliente privato in ambito sanitario. Voglio che la Ai identifichi possibili cause mediche di supporto al dottore. Che documenti devo preparare e avere o informazioni per essere compliance?

- La tua soluzione è AI sanitaria di supporto decisionale: NON può diagnosticare né decidere, il medico resta sempre responsabile, devi preparare documentazione tecnica, clinica, etica e di governance, la compliance si gioca su ruolo, rischio, supervisione umana e dati. Se salti i documenti giusti → rischio normativo serio.

1. Inquadramento (contesto + assunzioni) Assumo che: il cliente sia privato (clinica, azienda health, startup), l'AI: analizza dati clinici/sintomi, suggerisce possibili cause o ipotesi, supporta il medico, non il paziente direttamente, nessuna decisione automatica viene presa. ➡️ In AI Act sei provider (sviluppi la soluzione) ➡️ Il cliente è deployer ➡️ Il sistema è AI ad alto rischio (sanitario).
2. Riferimenti normativi (ancore chiave) AI Act – Reg. (UE) 2024/1689 [[Reg2024-1689 Art.6]] – sistemi AI ad alto rischio [[Reg2024-1689 Annex.III p.4]] – AI in ambito sanitario [[Reg2024-1689 Art.9]] – gestione del rischio [[Reg2024-1689 Art.10]] – governance dei dati [[Reg2024-1689 Art.11]] – documentazione tecnica [[Reg2024-1689 Art.14]] – supervisione umana [[Reg2024-1689 Art.22]] – responsabilità del provider Legge italiana 132/2025 [[L132 Art.7]] – uso dell'AI in ambito sanitario [[L132 Art.8]] – ricerca e sperimentazione clinica [[L132 Art.9]] – dati personali sanitari [[L132 Art.13]] – professioni intellettuali Codice Deontologico CNI [[CNI 4.1]] – responsabilità non delegabile [[CNI 6.2]] – responsabilità sugli effetti dell'AI [[CNI 3.3]] – tutela della salute e sicurezza
3. Classificazione del sistema (fondamentale) Il tuo sistema è: ✔ AI ad alto rischio (sanità, supporto clinico) ❌NON dispositivo medico autonomo (se resta supporto) ❌NON sistema diagnostico automatico 👉Questa distinzione deve essere scritta e dimostrabile.
4. Documenti OBBLIGATORI da preparare (core compliance)1️⃣ Documento di definizione del sistema (obbligatorio – base di tutto) Contiene: finalità clinica ammessa cosa FA e cosa NON FA il sistema esplicita frase tipo: "Il sistema non fornisce diagnosi né decisioni cliniche" 📌 Ancora: [[Reg2024-1689 Art.11]]2️⃣ Risk Management File (AI Risk Assessment) Devi: identificare rischi clinici (falsi positivi, omissioni, bias), valutare impatto su paziente e medico, definire mitigazioni. 📌Obbligatorio per AI ad alto rischio Ancora: [[Reg2024-1689 Art.9]]3️⃣ Documento di Supervisione Umana Deve spiegare: quando il medico interviene, cosa succede se il medico non è d'accordo, come l'AI può essere ignorata o spenta. 👉Il medico deve poter sempre dissentire. 📌 Ancora: [[Reg2024-1689 Art.14]]4️⃣ Governance dei dati sanitari Documento separato che descrive: origine dei dati (clinici, letteratura, linee guida), qualità, aggiornamento, rappresentatività, gestione bias, separazione training / test / uso reale. 📌 Ancora: [[Reg2024-1689 Art.10]], [[L132 Art.9]]5️⃣ Documentazione tecnica del modello / agenti Include: architettura multi-agente, logiche di orchestrazione, limiti noti, condizioni di fallimento. 📌 Ancora: [[Reg2024-1689 Art.11]]
5. Documenti CONTRATTUALI e LEGALI (essenziali)6️⃣ Clausola contrattuale con il cliente Deve dire chiaramente: che l'AI è strumento di supporto, che la responsabilità clinica è del medico, che il deployer garantisce uso conforme. 📌 Collegata a [[Reg2024-1689 Art.22]]7️⃣ Informativa per medici utilizzatori (trasparenza professionale) Deve spiegare: limiti del sistema, rischi residui, corretto uso. 📌 [[Reg2024-1689 Art.13]] + [[Reg2024-1689 Art.14]]
6. Evidenze operative da conservare Registro versioni modello Log delle raccomandazioni AI Tracce di decisione umana Report di test e validazione Verbali con clinici 👉 Servono prima, non dopo un incidente.
7. Errori GRAVI da evitare (linea rossa) 🔴Vietato di fatto: chiamarla "diagnosi" output visibili direttamente al paziente ranking automatico delle patologie senza contesto assenza di medico nel loop addestramento con dati clinici non governati Questi portano: violazione AI Act, possibile responsabilità professionale, rischio penale (fuori dal mio perimetro, ma reale).
8. Cosa ti consiglio come approccio pratico 👉 Design pattern corretto: "Clinical Decision Support – hypothesis generation" output = possibili ipotesi sempre accompagnate da: livello di confidenza, fonti cliniche, avvertenza esplicita.

16

Esempi: ti chiedo di fare un documento che rende conforme il progetto di cui al repo github https://github.com/smclab/openk9 **250k LOC** Analizzalo attentamente e poi scrivimi il dociumento o i documenti necessari in pdf o md - **Dopo MOLTI MINUTI:**

- Creerò tre documenti di conformità: un dossier sull'AI Act per OpenK9, una policy di uso accettabile e trasparenza, e una procedura di gestione degli incidenti. Potrei anche includere un template DPIA, ma fornirò solo un suggerimento legale. I documenti saranno disponibili in formato MD e PDF, e linkati per il download.
- Aprire la pagina del repository e il sito docs. Non sarebbe strettamente necessario fare uno screenshot per le immagini, ma dovrei seguire le istruzioni che richiedono uno screenshot durante l'analisi dei PDF. Ho già estratto il testo, ma se devo confermare alcune caratteristiche, farò degli screenshot delle pagine per essere conforme alle indicazioni.

```
TL;DR
 Ho analizzato le info pubbliche disponibili su OpenK9 (repo + sito/brochure) e ti ho preparato un pacchetto documentale “pronto all’uso” per impostare la conformità AI Act + Legge 132/2025, con classificazione ruolo/rischio, policy trasparenza, registro casi d’uso, incident handling, RACI, e addendum HIGH-RISK “se ricadi in Annex III”. Ho generato sia .md sia .pdf. • OpenK9 è descritto come cognitive enterprise search con ML per enrichment e opzioni GenAI / conversational search (chat su dati indicizzati).   • Non posso “certificare” la conformità solo dai sorgenti pubblici: la conformità dipende da come lo usi (es. HR, servizi essenziali, PA, ecc.) e da quali moduli AI abiliti. • Ho quindi prodotto un documento “compliance pack” che ti fa scegliere ruolo e rischio e ti dà checklist/evidenze.
```

```
Inquadramento (contesto + assunzioni)
```

Questa è un'analisi tecnico-normativa operativa, non un parere legale. Per decisioni ad alto impatto valida con legale/compliance. 3. Riferimenti con ancore (principali, usati nel documento)

```
•          [[Reg2024-1689 Art.3 c.0]], [[Reg2024-1689 Art.4]]
•          [[Reg2024-1689 Art.6 c.1]], [[Reg2024-1689 Art.6 c.2]], [[Reg2024-1689 Art.6 c.3]]
•          [[Reg2024-1689 Art.50 c.1]], [[Reg2024-1689 Art.50 c.2]], [[Reg2024-1689 Art.50 c.4]]
•          [[Reg2024-1689 Art.9 c.1]], [[Reg2024-1689 Art.10 c.1]], [[Reg2024-1689 Art.11 c.1]], [[Reg2024-1689 Art.12 c.1]], [[Reg2024-1689 Art.13 c.1]], [[Reg2024-1689 Art.14 c.1]], [[Reg2024-1689 Art.15 c.1]]
•          [[Reg2024-1689 Annex.III p.4]], [[Reg2024-1689 Annex.III p.5]], [[Reg2024-1689 Annex.IV p.2]]
•          [[L132 Art.1 c.2]], [[L132 Art.8 c.6]], [[L132 Art.24 c.2.d]], [[L132 Art.24 c.5.a]]
```

17

SEGUE

```
4.         Interpretazione operativa (cosa significa “nella vita vera”)

           •          Se abiliti “conversational search” devi mettere avvisi UI: l’utente deve sapere che interagisce con IA (Art.50).
           •          La parte “high-risk” non è automatica: scatta soprattutto se OpenK9 viene usato per HR/recruiting o per servizi essenziali/ammissibilità (Annex III).
           •          La Legge 132/2025 ti “riporta” all’AI Act e alle autorità competenti (anche privacy/Garante).

           5.         Cosa fare (checklist: oggi / 30 giorni / 90 giorni)
Nel documento trovi già la checklist; in sintesi:

           •          Oggi: inventario casi d’uso + scelta ruolo (provider/deployer) + avvisi trasparenza UI (se chat)
           •          30 giorni: policy uso accettabile + logging/monitoring + runbook incidenti
           •          90 giorni: risk assessment formale + test sicurezza (prompt injection / data leakage / multi-tenant) + formazione AI (Art.4)

           6.         Evidenze da conservare
Nel documento: registro casi d’uso, log, test report, screenshot avvisi, registro formazione, registro incidenti.
           7.         Rischi & errori tipici

           •          “È solo search” → poi lo usi in HR o servizi essenziali e diventa Annex III senza accorgertene.
           •          Attivi GenAI senza trasparenza e senza hardening contro leakage/prompt injection.
           •          Nessun owner/responsabilità: non sai chi decide change e chi firma il rischio.

           8.         Domanda successiva (una sola, decisiva)
OpenK9 lo userai anche per processi tipo HR (CV/assunzioni/valutazioni) o ammissibilità a servizi/benefit/credito, oppure “solo” come ricerca documentale interna?

——

File pronti
           •          Download del documento Markdown
           •          Download del PDF
```

18

SEGUE - doc di 6 pp

OpenK9 — Pacchetto documentale di conformità (AI Act + Legge 132/2025)

Versione: 0.1 (bozza operativa)

Data: 2026-01-31

Documento operativo tecnico-normativo, non parere legale.

*Va adattato al **contesto d'uso reale**, al **ruolo** (provider/deployer) e ai **moduli AI** effettivamente abilitati.*

---

1) Scopo e perimetro

Questo pacchetto serve a **rendere documentabile** (e verificabile) la conformità del progetto basato su **OpenK9** rispetto a:

- Regolamento (UE) 2024/1689 (AI Act)
- Legge italiana 23/09/2025 n.132 (attuazione/contesto nazionale)
- Doveri professionali (Codice Deontologico CNI) per chi progetta/integra/gestisce il sistema.

OpenK9 è descritto come **cognitive enterprise search** con **machine learning per arricchimento** e opzioni **GenAI / conversational search** (chat sui dati indicizzati).

Riferimenti progetto: README GitHub e sito OpenK9. (Vedi "Fonti di progetto" in fondo).

---

2) Classificazione: ruolo e rischio (decisione documentata)

2.1 Ruolo (chi sei tu rispetto a OpenK9?)

19

Domande da voi?

20

Grazie per l'attenzione!

Contatti

Francesco Marinuzzi

Whatsup. 348 65 42 168

Tel. 06 45 22 18 27 1

Email: info@marinuzzi.it

21

Human28: Il Futuro dell'AI con l'Uomo al Centro - Chi vuole unirsi?

Human28 con la vocazione di diventare leader nel settore dell'intelligenza artificiale, grazie al suo approccio innovativo che riporta l'elemento umano al centro dello sviluppo tecnologico.

Missione

Sviluppare agenti intelligenti che amplificano le capacità umane senza sostituirle, creando una sinergia uomo-macchina senza precedenti.

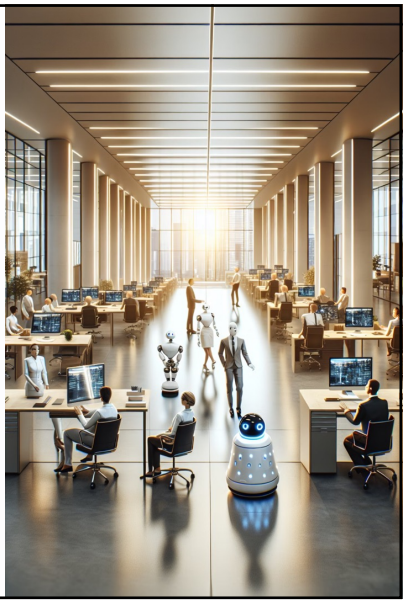
Visione

Un futuro in cui l'intelligenza artificiale potenzia la creatività, l'intuizione e l'empatia umana, elementi insostituibili nel processo decisionale.

Innovazione

Tecnologie proprietarie che permettono agli agenti AI di apprendere dalle interazioni umane, preservando il fattore umano in ogni fase del processo lavorativo.

Nel panorama dell'indistinguibilità tra umano e digitale del 2028, Human28 rappresenta il punto di equilibrio che garantisce che la tecnologia rimanga uno strumento al servizio dell'umanità.



22