PMI Digital Lab

GUIDA OPERATIVA 2026

AI Act per PMI

La guida pratica per censire gli strumenti AI, valutare i rischi e costruire un sistema di governance conforme all'AI Act.

Cosa troverai in questa guida

- ✓ Checklist compilabili
- ✓ Modelli pronti
- ✓ Caso pratico
- ✓ Piano operativo 30-60-90 giorni
- ✓ Registro AI

Una guida costruita per passare all’azione

Otto capitoli: dai concetti essenziali ai modelli operativi.

01 Cos’è davvero l’AI Act 03

02 Chi riguarda 06

03 I quattro livelli di rischio 09

04 Checklist di conformità 13

05 Caso pratico 19

06 Errori più comuni 23

07 Modelli pronti 26

08 Piano operativo 31

01

Perché l'AI Act riguarda anche la tua PMI

Il Regolamento (UE) 2024/1689 crea regole uniformi per il mercato europeo.

01

Approccio basato sul rischio

Più un sistema può incidere su salute, sicurezza o diritti fondamentali, più aumentano gli obblighi.

02

Responsabilità lungo la filiera

Fornitori, deployer, importatori e distributori hanno compiti differenti.

03

Documentazione e controllo

La conformità richiede evidenze, ruoli, procedure e monitoraggio, non una semplice dichiarazione.

Esempi di sistemi AI utilizzati nelle PMI

ChatGPT
Microsoft Copilot
Google Gemini
Claude
Make
Zapier
Notion AI
Perplexity

Se utilizzi uno o più di questi strumenti, questa guida ti aiuterà a organizzarne l'uso in modo più consapevole.

IDEA CHIAVE

La conformità non parte dalla tecnologia, ma dal modo in cui la tua azienda utilizza l'intelligenza artificiale. Per questo ogni sistema AI deve essere identificato, classificato e documentato in base al suo utilizzo concreto.

AI Act e GDPR: perché servono entrambi nella tua azienda

La conformità deve integrare governance dell’AI, privacy, sicurezza e lavoro.

AI Act	GDPR
Regola i sistemi di AI	Regola il trattamento dei dati personali
Valuta il livello di rischio	Valuta la liceità del trattamento
Definisce obblighi sull'uso dell'AI	Definisce obblighi sulla protezione dei dati
Si applica anche senza dati personali	Si applica solo se sono trattati dati personali

Esempio pratico

Un dipendente utilizza ChatGPT per preparare una bozza di email.

AI Act

↓

Valuto come viene utilizzato il sistema AI.

GDPR

↓

Valuto se vengono inseriti dati personali e come vengono trattati.

ATTENZIONE

Essere conformi al GDPR non significa essere automaticamente conformi all'AI Act. Le due verifiche devono essere svolte insieme.

- Nel Capitolo 4 troverai una checklist per verificare entrambi gli aspetti durante l'adozione di nuovi strumenti AI.

Quando entra in vigore l'AI Act e cosa significa per la tua PMI

Le principali tappe dell'AI Act e le attività che una PMI dovrebbe pianificare per tempo.

2 febbraio 2025

- Pratiche vietate
- Alfabetizzazione AI

Cosa dovrebbe fare una PMI

2 febbraio 2025

- ✔️ Verificare se vengono utilizzati sistemi AI.
- ✔️ Evitare pratiche vietate.
- ✔️ Avviare la formazione interna.

2 agosto 2025

- Governance
- Modelli AI per finalità generali

2 agosto 2025

- ✔️ Identificare i fornitori AI.
- ✔️ Verificare documentazione e contratti.

2 agosto 2026

Applicazione della maggior parte delle disposizioni

2 agosto 2026

- ✔️ Completare inventario AI.
- ✔️ Formalizzare ruoli.
- ✔️ Aggiornare policy.
- ✔️ Attivare il monitoraggio.

Nota importante
Le date rappresentano le principali tappe dell'AI Act. Prima di assumere decisioni operative o legali, verifica sempre il testo vigente e le linee guida ufficiali.

Per capire gli obblighi dell'AI Act devi prima identificare il tuo ruolo.

02

Per applicare correttamente l'AI Act, la prima domanda da porti non è quale strumento utilizzi, ma quale ruolo ricopre la tua azienda rispetto a quel sistema AI.

🧩 Fornitore

Sviluppa un sistema AI o lo fa sviluppare e lo immette sul mercato o in servizio con il proprio nome o marchio.

Esempio: sviluppi o commercializzi un software AI con il tuo marchio.

💼 Deployer

Utilizza un sistema AI sotto la propria autorità, salvo gli utilizzi personali non professionali.

Esempio: utilizzi ChatGPT o Copilot nelle attività della tua azienda.

Una stessa PMI può essere deployer e fornitore contemporaneamente, ma rispetto a sistemi o casi d’uso differenti. Il ruolo deve quindi essere verificato per ogni singolo sistema AI.

In alcuni casi, modificare sostanzialmente un sistema o commercializzarlo con il proprio marchio può far assumere all’impresa gli obblighi del fornitore.

Nella pagina successiva vedremo tutti i ruoli previsti dall'AI Act e come identificarli nella pratica.

La stessa azienda può ricoprire ruoli diversi in base al sistema AI utilizzato o sviluppato.

La mappa dei ruoli evita di applicare obblighi generici o incompleti.

FORNITORE

Sviluppa o commercializza il sistema con il proprio nome o marchio.

Esempio: sviluppi o commercializzi un software AI con il tuo marchio.

DEPLOYER

Utilizza il sistema all'interno dell'attività professionale.

Esempio: utilizzi ChatGPT o Copilot nelle attività della tua azienda.

IMPORTATORE

Immette nell'Unione un sistema che reca il nome o marchio di un soggetto stabilito fuori dall'UE.

DISTRIBUTORE

Rende disponibile un sistema sul mercato senza essere fornitore o importatore.

Da ricordare

I ruoli non sono assegnati all'azienda, ma al rapporto che l'azienda ha con ciascun sistema AI.

Prima di classificare il rischio di un sistema AI, identifica sempre il ruolo che la tua azienda ricopre rispetto a quello specifico sistema.

Prima di classificare un sistema AI, rispondi a queste tre domande

La classificazione parte dall’attività reale, non dal nome commerciale dello strumento.

01

Che cosa fa realmente questo sistema AI?

Descrivere input, elaborazione, output e decisione supportata.

02

Su quali persone può avere un impatto?

Identificare dipendenti, candidati, clienti, fornitori o cittadini interessati.

03

Chi prende la decisione finale: il sistema o una persona?

Chiarire se l’output informa, raccomanda, ordina o produce direttamente un effetto.

Esempio

Strumento	**ChatGPT**
Finalità	**Bozze email**
Persone coinvolte	**Clienti**
Decisione finale	**Operatore**
Ruolo	**Deployer**

RISULTATO

Per ogni sistema AI utilizzato in azienda dovrebbe esistere una scheda che descriva finalità, persone coinvolte, ruolo dell'impresa e livello di rischio.

I quattro livelli di rischio previsti dall'AI Act

03

La categoria determina divieti, requisiti, trasparenza o buone pratiche.

01	**INACCETTABILE**	Quando? Pratiche espressamente vietate dal regolamento.	**Vietato**
02	**ALTO**	Quando? Il sistema è utilizzato in uno degli ambiti ad alto rischio previsti dall'AI Act	**Obblighi rigorosi**
03	**LIMITATO**	Quando? È richiesto un obbligo di trasparenza verso gli utenti.	**Obblighi di trasparenza**
04	**MINIMO O NULLO**	Quando? Il caso d'uso non rientra nelle categorie precedenti.	**Nessun obbligo specifico**

Da ricordare

Prima identifica il ruolo della tua azienda. Poi valuta il caso d'uso. Solo a questo punto puoi classificare il livello di rischio del sistema AI.

Le pratiche vietate richiedono un intervento immediato

Le pratiche vietate non possono essere “mitigate” con una policy interna.

01

Individua

Cerca usi che manipolano, sfruttano vulnerabilità o applicano forme vietate di classificazione e sorveglianza.

02

Interrompi immediatamente l'utilizzo

Sospendi l’uso quando il caso rientra in un divieto applicabile.

03

Documenta

Registra l'analisi svolta, la decisione presa, il responsabile e le misure adottate.

Nella maggior parte delle PMI, le pratiche vietate sono poco frequenti. Tuttavia è importante verificarne l'assenza durante il censimento iniziale dei sistemi AI.

!

ATTENZIONE

Le pratiche vietate sono definite direttamente dall'AI Act. In caso di dubbio, verifica sempre il testo del regolamento e le linee guida ufficiali prima di assumere decisioni operative.

L’alto rischio dipende dalla funzione e dal contesto

Il semplice uso di un prodotto noto non determina da solo la categoria.

ESEMPI DI AMBITI

- Occupazione e gestione dei lavoratori; istruzione;
- accesso a servizi essenziali;
- biometria;
- infrastrutture critiche;
- alcuni utilizzi in giustizia e migrazione.

VERIFICHE

- Finalità prevista;
- categoria dell’Allegato III;
- eventuali esclusioni;
- ruolo dell’impresa;
- uso effettivo;
- impatto sulle persone.

Verifica consigliata

Se un sistema AI può incidere su diritti, opportunità o decisioni rilevanti per le persone, è opportuno effettuare una verifica specialistica prima dell'utilizzo.

Rischio limitato non significa assenza di obblighi

Alcuni sistemi richiedono trasparenza verso le persone o sui contenuti generati.

01

Interazione con persone

Informare chiaramente quando una persona sta interagendo con un sistema AI, nei casi previsti dal regolamento.

02

Contenuti generati o modificati con l'AI

Gestire correttamente marcatura o comunicazione per contenuti generati o manipolati.

03

Procedure interne

Definire modelli di informativa, responsabilità e controlli prima della pubblicazione.

i

DA RICORDARE

Aggiungere la verifica di trasparenza alla checklist di approvazione dei contenuti.

La conformità parte da otto controlli documentabili

04

Prima verifica operativa per una PMI.
Nelle pagine seguenti ogni controllo viene approfondito con una checklist dedicata.

Inventario AI

Strumenti, finalità, responsabili e dati.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Valutazione rischio

Categoria e motivazione documentata.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Informativa

Trasparenza verso utenti e interessati.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Supervisione umana

Chi controlla, approva o interrompe.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Registro interno

Decisioni, incidenti e revisioni.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Formazione

Competenze adeguate ai ruoli.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Sicurezza

Accessi, dati e fornitori.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Monitoraggio

Prestazioni, errori e cambiamenti.

□ Non avviato
□ In corso
□ Completato

NOTE _____

DA RICORDARE

Completare stato e note per ogni requisito; assegnare owner e data di riesame.

Inventario e valutazione devono essere collegati

Ogni riga dell’inventario deve condurre a una decisione sul rischio.

Nome e versione

Prodotto, modello e piano utilizzato.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Processo

Attività aziendale supportata.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Finalità

Problema risolto e risultato atteso.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Dati

Categorie di dati inserite o accessibili.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Persone

Soggetti potenzialmente interessati.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Ruolo

Fornitore, deployer o altro.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Rischio

Categoria e motivazione.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Responsabile

Owner e approvatore interno.

□ Non avviato
□ In corso
□ Completato

NOTE _____

i

DA RICORDARE

Verifica che ogni sistema AI abbia una motivazione documentata per la classificazione del rischio.

Trasparenza e supervisione si progettano nel processo

Una formula generica non sostituisce un controllo realmente applicabile.

Avviso utente

Quando e come informare.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Etichettatura

Contenuti generati o manipolati.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Punto di controllo

Dove interviene una persona.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Autorità

Chi può approvare o rifiutare.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Escalation

Quando fermare il flusso.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Tracciabilità

Quali prove conservare.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Contestazione

Come gestire una segnalazione.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Accessibilità

Informazioni chiare e comprensibili.

□ Non avviato
□ In corso
□ Completato

NOTE _____

DA RICORDARE

La supervisione umana deve essere definita prima della messa in esercizio del processo.

Il registro interno rende le decisioni verificabili

Registrare ciò che è utile a ricostruire uso, cambiamenti e controlli.

Data e autore

Chi ha effettuato la registrazione.

□ Non avviato

□ In corso

□ Completato

NOTE _____

Decisione

Scelta presa e motivazione.

□ Non avviato

□ In corso

□ Completato

NOTE _____

Versione

Sistema, modello o configurazione.

□ Non avviato

□ In corso

□ Completato

NOTE _____

Output da verificare

Risultato che richiede verifica.

□ Non avviato

□ In corso

□ Completato

NOTE _____

Errore

Problema riscontrato.

□ Non avviato

□ In corso

□ Completato

NOTE _____

Azione correttiva

Misura adottata.

□ Non avviato

□ In corso

□ Completato

NOTE _____

Approvazione

Responsabile della chiusura.

□ Non avviato

□ In corso

□ Completato

NOTE _____

Riesame

Data della verifica successiva.

□ Non avviato

□ In corso

□ Completato

NOTE _____

DA RICORDARE

Il registro interno è utile solo se viene aggiornato con regolarità.

Formazione e sicurezza sono controlli permanenti

Le competenze devono essere adeguate al ruolo e al rischio del caso d’uso.

Ruoli formati

Utenti, owner, IT, HR e direzione.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Strumenti autorizzati

Attività e strumenti approvati.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Dati vietati

Informazioni da non inserire.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Verifica output

Errori, bias e allucinazioni.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Accessi

Account nominativi e privilegi minimi.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Fornitori

Contratti e impostazioni verificate.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Incidenti

Canale e tempi di segnalazione.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Aggiornamenti

Formazione dopo cambiamenti rilevanti.

□ Non avviato
□ In corso
□ Completato

NOTE _____

i

DA RICORDARE

La formazione deve seguire anche gli aggiornamenti degli strumenti AI adottati.

Il monitoraggio chiude il ciclo di conformità

Controllare non solo il sistema, ma anche processo, persone e fornitore.

Qualità degli output

Accuratezza e adeguatezza.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Eccezioni

Casi non gestiti correttamente.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Reclami

Segnalazioni di utenti o dipendenti.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Cambiamenti

Nuove funzioni, modelli o integrazioni.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Utilizzi impropri

Shadow AI e deviazioni dalla policy.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Incidenti

Impatto, causa e risposta.

□ Non avviato
□ In corso
□ Completato

NOTE _____

KPI

Indicatori proporzionati al rischio.

□ Non avviato
□ In corso
□ Completato

NOTE _____

Riesame

Cadenza e responsabile.

□ Non avviato
□ In corso
□ Completato

NOTE _____

i

DA RICORDARE

Pianifica un riesame periodico dell'inventario e delle classificazioni.

Una PMI di 35 dipendenti utilizza tre strumenti in processi diversi

05

Caso ipotetico: azienda di servizi B2B con funzioni commerciali, amministrative e operative.

01

ChatGPT

Marketing e comunicazione

Bozze email, sintesi di documenti e ideazione di contenuti.

02

Microsoft Copilot

Produttività interna

Supporto in Word, Excel, Outlook e Teams.

03

Make

Make è una piattaforma di automazione e non ogni automazione realizzata con Make è necessariamente un sistema AI.

Automazioni tra moduli, CRM, email e fogli di calcolo, anche con eventuali funzioni AI integrate.

i

OBIETTIVO

Valutare separatamente ogni caso d’uso, considerando finalità, dati, persone interessate e controlli applicabili.

L’inventario separa strumenti, usi e dati trattati

Lo stesso prodotto può contenere casi d’uso con profili di rischio diversi.

01

ChatGPT — marketing

Bozze di post con informazioni pubbliche.
Owner: Marketing.
Non inserire dati personali.

02

Copilot — riunioni

Sintesi di meeting interni. Owner:
Operations.
Verificare accessi e conservazione dei dati.

03

Make — lead

Trasferimento dati dal modulo al CRM.
Owner: Sales Ops.
Log ed errori da monitorare.

***Owner = responsabile del processo o dell'attività.**

i

RISULTATO

Tre casi d'uso distinti, non una sola voce generica “strumenti AI”.

La valutazione distingue produttività e decisioni sulle persone

Il livello di attenzione cresce quando l’output influenza diritti, accesso o valutazioni.

Caso d'uso a rischio contenuto

Bozze marketing su contenuti pubblici, sempre revisionate prima della pubblicazione.

Controlli: accuratezza, copyright, tono e approvazione umana.

Esempio:
ChatGPT prepara una prima bozza di un post LinkedIn utilizzando solo informazioni pubbliche. Un responsabile marketing verifica e approva il testo prima della pubblicazione.

Priorità più alta

Uso dell’AI per selezionare candidati, valutare prestazioni o decidere accesso a servizi.

Richiede analisi specifica e coinvolgimento di funzioni competenti.

Esempio:
Un sistema AI assegna un punteggio ai candidati e determina quali profili passano alla fase successiva del processo di selezione.

Da valutare prima dell’uso: finalità, dati, impatto sulle persone, supervisione umana e obblighi applicabili.

DECISIONE

Non introdurre nuovi utilizzi dell'AI nei processi HR senza una valutazione preventiva.

Procedure e monitoraggio trasformano l’inventario in governance

Il caso ipotetico adotta cinque controlli semplici e verificabili.

01

Approvazione strumenti

Solo account e piani autorizzati.

02

Regole sui dati

Non inserire dati riservati nei servizi AI non approvati dall'azienda.

03

Revisione umana

Output verificato prima di invio, pubblicazione o decisione.

04

Registro incidenti

Errori, divulgazioni e automazioni fallite sono registrati.

05

Riesame trimestrale

Owner, IT e direzione aggiornano inventario e priorità.

06

Errore 1: creare una policy senza sapere quali strumenti sono usati

Una policy generica non individua rischi, responsabili o dati.

PERCHÉ NON FUNZIONA

Non intercetta Shadow AI, integrazioni, account personali o funzionalità introdotte dagli aggiornamenti.

COME CORREGGERE

Avviare un inventario leggero per reparto e collegarlo a owner, finalità, dati e frequenza di riesame.

***Owner = responsabile del processo o dell'attività.**

ESEMPIO CONCRETO

Un’azienda approva una policy generica sull’AI, ma non censisce gli utilizzi reali. Il reparto commerciale usa ChatGPT con account personali, mentre un’automazione in Make trasferisce i dati dei lead nel CRM.
La policy non intercetta quindi **Shadow AI, account non autorizzati, integrazioni, dati trattati e responsabilità interne.**

Prima si censiscono strumenti e casi d’uso; solo dopo si definiscono regole efficaci.

BEST PRACTICE

Raccogliere prima i casi d’uso, poi scrivere regole aderenti alla realtà aziendale.

Errore 2: classificare il rischio solo in base al nome del prodotto

ChatGPT, Copilot o Make non hanno un unico livello di rischio.

PERCHÉ NON FUNZIONA

IUno stesso strumento AI può essere utilizzato per attività molto diverse. Preparare una bozza di testo non ha lo stesso impatto che valutare un candidato, assegnare una priorità a un cliente o supportare una decisione che riguarda una persona. Per questo il livello di rischio non può essere stabilito soltanto guardando il nome del prodotto.

COME CORREGGERE

Valuta separatamente ogni caso d’uso. Per ciascuno descrivi che cosa fa il sistema, quali dati utilizza, quali persone possono essere coinvolte e quale decisione viene presa sulla base dell’output. Solo dopo queste verifiche puoi determinare quali obblighi e controlli applicare.

ESEMPIO

Un’azienda utilizza ChatGPT per preparare una prima bozza della newsletter mensile. Il testo viene sempre controllato dal responsabile marketing prima della pubblicazione.
La stessa azienda vorrebbe usare ChatGPT anche per confrontare i curriculum e suggerire quali candidati convocare. In questo secondo caso l’output può influenzare concretamente un’opportunità di lavoro e richiede quindi una valutazione molto più approfondita.

ATTENZIONE

Un utilizzo inizialmente semplice può diventare più delicato quando viene collegato a un processo decisionale o utilizzato per produrre effetti sulle persone.

Errore 3: affidarsi al fornitore e dimenticare il processo interno

Le garanzie del prodotto non sostituiscono controlli, formazione e supervisione.

PERCHÉ NON FUNZIONA

Anche quando il fornitore offre garanzie di sicurezza e conformità, l'azienda resta responsabile di come configura il sistema, dei dati che inserisce, di chi può utilizzarlo e delle decisioni prese sulla base degli output.

COME CORREGGERE

Definire responsabili, approvazioni, procedure di escalation, registrazione delle attività, monitoraggio e criteri per sospendere l'utilizzo quando necessario.

ESEMPIO

Un'azienda acquista ChatGPT Enterprise pensando che questo sia sufficiente per essere conforme. Tuttavia non definisce chi può utilizzarlo, quali dati possono essere inseriti, chi verifica gli output e come gestire eventuali errori.

Il fornitore mette a disposizione lo strumento, ma la gestione quotidiana e i controlli restano responsabilità dell'azienda.

CONSIGLIO

Inserire la verifica del fornitore nel processo di acquisto e ripeterla quando il servizio o il sistema AI subiscono cambiamenti rilevanti.

07

Registro AI

Compila una scheda separata per ogni sistema AI utilizzato in azienda.

Strumento / versione / fornitore

Processo e finalità d’uso

Ruolo dell’impresa e responsabile del processo

Categoria di rischio e motivazione

Dati trattati e persone interessate

Ultima revisione (data ultimo aggiornamento): _____ / _____ / _____

Stato: □ Attivo □ In valutazione □ Sospeso □ Dismesso

Documenti collegati: □ Valutazione del rischio □ Policy AI □ Registro Prompt □ Procedura interna

i

ISTRUZIONE

Compila una scheda per ogni sistema AI o caso d'uso significativo. Aggiornala ogni volta che cambiano finalità, dati trattati, configurazione o responsabili.

Registro Prompt

Compila questa scheda per ogni caso d'uso AI che richiede una valutazione del rischio. Documentare il ragionamento aiuta a dimostrare il processo seguito e facilita gli aggiornamenti futuri.

ID prompt / data / autore

Strumento e versione

Testo o struttura del prompt

Dati ammessi e dati vietati

Criterio di verifica dell'output

Ultima revisione (data ultimo aggiornamento): _____ / _____ / _____

Valutazione eseguita da: _____

Prossima revisione: _____ / _____ / _____

Documenti di supporto: □ Registro AI □ Policy AI □ Documentazione del fornitore □ Procedura interna

ISTRUZIONE

Rivedi questa valutazione ogni volta che cambiano finalità del sistema, dati trattati, modalità di utilizzo, funzionalità disponibili o impatto sulle persone.

Inventario AI

Utilizza questa checklist per verificare che il sistema AI sia stato configurato correttamente prima della messa in produzione e durante le verifiche periodiche.

Reparto / processo / responsabile del processo

Strumento / piano / account

Caso d’uso e frequenza

Integrazioni e fonti dati

Stato: approvato / limitato / sospeso

Data della verifica: _____ / _____ / _____

Verifica eseguita da: _____

Esito della verifica: ☐ Conforme ☐ Conforme con azioni correttive ☐ Non conforme

Azioni correttive:

---

i

ISTRUZIONE

Compila questa checklist prima dell'attivazione del sistema AI. Aggiornala quando vengono introdotte nuove funzionalità, cambiano i dati trattati o viene modificato il processo aziendale. Conserva la checklist insieme al Registro AI.

Valutazione fornitori

Utilizza questa scheda per valutare ogni fornitore di sistemi AI prima dell'acquisto, del rinnovo del contratto o dell'introduzione di nuove funzionalità.

Identità, sede e subfornitori

Termini, ruoli privacy e uso dei dati

Sicurezza, accessi e conservazione

Documentazione AI Act disponibile

Incidenti, assistenza e diritto di audit

Nome del fornitore: _____

Servizio / Sistema AI: _____

Data della valutazione: _____ / _____ / _____

Valutazione eseguita da: _____

Esito della valutazione: □ Approvato □ Approvato con condizioni □ Non approvato

Azioni richieste:

ISTRUZIONE

Compila questa scheda per ogni fornitore di sistemi AI utilizzato dall'azienda. Aggiornala quando cambiano il contratto, le funzionalità disponibili, le condizioni di utilizzo o vengono introdotti nuovi trattamenti di dati. Conserva la scheda insieme al Registro AI.

Procedura interna

Utilizza questo modello come base per definire una procedura interna sulla gestione dei sistemi di intelligenza artificiale. Personalizzalo in base ai processi e all'organizzazione della tua azienda.

Scopo, ambito e definizioni

Ruoli e responsabilità

Richiesta e approvazione di nuovi usi

Regole operative e supervisione

Incidenti, monitoraggio e riesame

Nome della procedura: _____

Versione: _____ **Data di emissione:** _____ / _____ / _____

Responsabile della procedura: _____

Approvazioni

Redatta da: _____ **Verificata da:** _____ **Approvata da:** _____

Data: _____ / _____ / _____ **Prossimo riesame:** _____ / _____ / _____

Documenti collegati

☐ Registro AI ☐ Registro Prompt ☐ Inventario AI ☐ Valutazione fornitori ☐ Policy AI

ISTRUZIONE

Personalizza questa procedura in base all'organizzazione aziendale. Aggiornala quando cambiano processi, sistemi AI utilizzati, ruoli, responsabilità o requisiti normativi. Conserva ogni versione per mantenere la tracciabilità delle modifiche.

Primi 30 giorni: vedere e mettere ordine

08

Obiettivo: ottenere una visione completa dei sistemi AI già utilizzati in azienda, definire le prime responsabilità e individuare le situazioni che richiedono un intervento prioritario.

01 **Nomina il coordinatore**

Una persona raccoglie informazioni e coinvolge direzione, IT, HR, privacy e process owner.

02 **Crea l’inventario**

Censisci strumenti ufficiali, account individuali, integrazioni e automazioni.

03 **Blocca gli usi evidenti**

Sospendi pratiche non autorizzate o dati riservati in servizi non approvati.

04 **Avvia la formazione**

Spiega regole minime, rischi e canale per chiedere assistenza.

Responsabile del piano

Data di avvio: _____ / _____ / _____ **Data prevista di completamento:** _____ / _____ / _____

Stato di avanzamento

□ Non avviato □ In corso □ Completato

Evidenze raccolte

(documenti prodotti, inventario completato, policy redatte, altre evidenze di lavoro svolto)

RISULTATO ATTESO

Al termine dei primi 30 giorni l'azienda dovrebbe disporre di un inventario aggiornato dei sistemi AI utilizzati, dei responsabili coinvolti e delle principali aree che richiedono ulteriori verifiche. Questa documentazione costituirà la base per le attività previste nella fase successiva.

Entro 60 giorni: classificare e formalizzare

Obiettivo: trasformare l'inventario iniziale in un sistema organizzato di regole, responsabilità e controlli documentabili, definendo una governance AI proporzionata alle esigenze dell'azienda.

01 **Valuta i casi d’uso**

Ruolo, rischio, dati, persone interessate e supervisione.

02 **Definisci la policy**

Strumenti ammessi, divieti, approvazioni, regole sui dati e incidenti.

03 **Valuta i fornitori**

Contratti, sicurezza, documentazione e impostazioni.

04 **Crea registri**

Decisioni, prompt rilevanti, incidenti, revisioni e azioni correttive.

Responsabile del piano

Data di avvio: _____ / _____ / _____ **Data prevista di completamento:** _____ / _____ / _____

Stato di avanzamento

□ Non avviato □ In corso □ Completato

i

RISULTATO ATTESO

Al termine dei primi 60 giorni l'azienda dovrebbe aver classificato i principali casi d'uso AI, definito regole interne, verificato i fornitori e predisposto la documentazione essenziale per gestire l'intelligenza artificiale in modo organizzato e documentabile.

Evidenze raccolte

(documenti prodotti, inventario completato, policy redatte, altre evidenze di lavoro svolto)

Entro 90 giorni: misurare e migliorare

Obiettivo: trasformare la governance AI in un processo continuo di monitoraggio, verifica e miglioramento.

01

Monitora gli indicatori

Errori, incidenti, reclami, eccezioni e modifiche significative.

02

Esegui un riesame

Verifica inventario AI, classificazioni, policy, formazione e azioni correttive.

03

Verifica la gestione degli incidenti

Simula un output errato, una divulgazione di dati o un malfunzionamento per verificare la risposta dell'organizzazione.

04

Pianifica il miglioramento successivo

Assegna scadenze, budget e responsabilità per i prossimi 90 giorni.

Una governance efficace non termina con l'adozione delle regole: continua attraverso monitoraggio, riesami e miglioramento costante.

i

RISULTATO ATTESO

Al termine dei 90 giorni l'azienda dispone di responsabilità chiare, evidenze documentali aggiornate e un piano di miglioramento per il ciclo successivo.

Approfondisci e scarica i modelli operativi

SCANSIONA E ACCEDI ALLE RISORSE

QR articolo AI Act

QR Registro AI

QR AI Policy

QR articolo ISO 42001

NOTA DI PRODUZIONE

I quattro quadrati mantengono la stessa dimensione e lo stesso allineamento.

PMI Digital Lab

PROSSIMO PASSO

Porta la governance AI nella tua impresa

Scopri guide operative, checklist e modelli gratuiti pensati per aiutare le PMI italiane a gestire l’intelligenza artificiale in modo responsabile.

SCANSIONA E ACCEDI ALLE RISORSE

www.pmidigitallab.it

Approfondimenti pratici su AI Act, policy aziendali, Registro AI, valutazione dei rischi e organizzazione interna.

QR

Questa guida ha finalità informative e organizzative e non costituisce consulenza legale, tecnica o in materia di protezione dei dati.
Ogni impresa deve valutare il proprio caso concreto e, quando necessario, rivolgersi a professionisti qualificati.