

ESERCIZIO: ANALISI DI CONFORMITÀ SU UN CASO PRATICO



Tabella contenuti:

1. Identificare la categoria di rischio secondo l'EU Ai Act:	1
2. Individuare i principali requisiti di conformità applicabili:.....	1
3. Proporre le misure da implementare per rispettare gli obblighi legali e regolamentari:	2
4. Indicare come documentare e dimostrare la conformità:	2
5. (Opzionale) Individuare possibili criticità e suggerire miglioramenti:	2

1. Identificare la categoria di rischio secondo l'EU Ai Act:

Rilevato rischio limitato:

L'applicazione automatizza risposte su documenti aziendali senza prendere decisioni che impattano diritti o accesso a servizi. Non rientra tra i sistemi vietati o ad alto rischio, salvo usi specifici (es. HR, sanità).

2. Individuare i principali requisiti di conformità applicabili:

- Trasparenza: informare l'utente dell'uso di AI.
- Tracciabilità: tenere log delle interazioni.
- Privacy: rispettare GDPR per i dati trattati.
- Documentazione: descrivere modelli, flussi dati, gestione incidenti.

- DPIA e audit solo per usi sensibili

3. Proporre le misure da implementare per rispettare gli obblighi legali e regolamentari:

- Messaggio in UI che avvisa dell'uso di AI.
- Log di richieste e risposte.
- Policy privacy aggiornata, accesso limitato ai dati.
- Documentazione tecnica aggiornata.
- DPIA e audit se usato in contesti ad alto rischio.

4. Indicare come documentare e dimostrare la conformità:

- Registro log dettagliato delle attività.
- DPIA solo se necessario.
- User notice visibile e privacy policy aggiornata.
- Log sicuri e accessibili solo a personale autorizzato.

5. (Opzionale) Individuare possibili criticità e suggerire miglioramenti:

Se usato per decisioni sensibili, va rivalutato come alto rischio.

Rischio perdita dati se i documenti vanno su cloud.

Suggerimenti:

- Anonimizzare dati prima di inviarli al cloud
- Revisioni periodiche di policy e log
- Coinvolgere responsabile privacy in casi dubbi