

Conclusione

Valutazione dell'impatto della protezione dei dati (DPIA)

Una Pre-DPIA valuta se il trattamento dei dati personali previsto presenta un rischio elevato per l'interessato. A seconda della giurisdizione, delle dimensioni e della natura del progetto e della tipologia di dati da trattare, si dovrà determinare se sia necessaria una DPIA completa oppure no.

Una valutazione di impatto della protezione dei dati completa (DPIA) ha lo scopo di valutare i rischi per i diritti e le libertà degli interessati. Se richiesto dalle leggi o dai regolamenti locali, è necessario completare una DPIA quando si avvia un nuovo progetto, si introduce una nuova applicazione, un prodotto o un servizio esistente o lo si modifica in modo significativo con un elevato impatto sui dati personali.

Registri delle attività di trattamento (ROPA)

Il trattamento dei dati personali deve essere documentato nel Registro delle attività di trattamento (ROPA). Il documento specifica le categorie di dati personali trattati, dove e perché vengono conservati e chi vi ha accesso. Per ulteriori informazioni, contattate il team locale di Information Governance e Privacy o il team locale di Compliance.

I rischi legati all'utilizzo dell'intelligenza artificiale

L'utilizzo dell'IA comporta alcuni rischi che devono essere mitigati. Questi includono:

- Bias cognitivi e discriminazione: L'intelligenza artificiale può prendere decisioni solo in base ai dati a cui ha accesso e non in base al quadro completo della situazione.
- Mancanza di trasparenza: potrebbe essere difficile spiegare come vengono prese le decisioni, soprattutto quando non è previsto alcun intervento umano nel processo decisionale.
- Information Security: esiste la possibilità che grandi sistemi informatici vengano violati da attacchi informatici condotti da hacker, i quali potrebbero essere in grado di accedere a grandi volumi di dati personali.

Zurich opera in modo responsabile secondo i principi dell'IA responsabile, quali sicurezza, trasparenza, responsabilità e affidabilità.

Risk management framework

Oltre a lavorare secondo i principi dell'IA responsabile, il nostro utilizzo dell'IA è regolato dal nostro Risk management framework, che comprende le politiche sulla privacy dei dati e su Information Security, nonché la nostra AIAF Guidance. Questa guida incorpora le best practice del settore per valutare i sistemi di IA, fra le altre cose, in termini di accuratezza, spiegabilità ed equità durante il loro ciclo di vita.

Per ulteriori informazioni, contattate il vostro esperto locale di AI Governance o il team di Local Compliance.

Chi contattare

Contattate il vostro esperto locale di AI Governance o l'ufficio Compliance locale per qualsiasi domanda sull'IA.

