

IL DPO NELLA GESTIONE DEL PERSONALE: APPROCCIO OPERATIVO

AUTORE: **Elena Maderna**

Data Protection Manager – Gruppo San Donato



Milano, maggio 2025

- La gestione del personale implica un elevato trattamento di dati personali, rendendo cruciale la protezione delle informazioni.
- Il DPO assicura la conformità al GDPR e al Regolamento UE 2024/1689 sull'IA, mitigando i rischi legati a tali trattamenti.
- **L'uso dell'IA nei processi HR introduce nuove sfide come la discriminazione algoritmica e la trasparenza delle decisioni automatizzate.**
- Importanza della collaborazione tra DPO, dipartimento IT e HR per garantire una gestione responsabile e conforme dei dati.

RUOLO E RESPONSABILITA' DEL DPO

- Verifica della liceità del trattamento dati (art. 6 GDPR) e supporta il titolare nell'ambito delle basi giuridiche per la raccolta e l'uso dei dati.
- Principio di minimizzazione dei dati (art. 5 GDPR): raccolta solo delle informazioni necessarie e limitazione dei tempi di conservazione.
- **Sorveglianza sui sistemi di IA per la selezione e gestione del personale, con particolare attenzione ai bias e alla trasparenza degli algoritmi.**
- DPIA per trattamenti HR ad alto rischio (art. 35 GDPR), per valutare e mitigare i rischi per i diritti e le libertà dei dipendenti.
- Garanzia dei diritti degli interessati (artt. 15-22 GDPR), come il diritto di accesso, rettifica, opposizione, limitazione e cancellazione dei dati personali.

SORVEGLIANZA SUI SISTEMI DI SELEZIONE AUTOMATIZZATA

Un'azienda introduce un software basato su intelligenza artificiale per il reclutamento del personale. Il sistema analizza i CV e le interviste video dei candidati, **assegnando un punteggio a ciascun profilo in base a parametri prestabiliti**. Dopo un audit interno, il DPO scopre che l'algoritmo penalizza **sistematicamente i candidati con lacune linguistiche**, indipendentemente dalle competenze professionali richieste per il ruolo.

PROBLEMI INDIVIDUATI:

Bias algoritmico: il sistema è stato addestrato su un dataset non equilibrato, penalizzando alcuni gruppi di candidati.

Manca di trasparenza: il software non fornisce informazioni chiare sulle motivazioni dei punteggi assegnati.

Violazione del principio di equità: le decisioni automatizzate potrebbero costituire una forma di discriminazione indiretta.

SOLUZIONI OPERATIVE

Verificare che il modello di IA sia stato addestrato su **dataset diversificati**, rappresentativi di una popolazione ampia ed equa.

Richiedere **trasparenza ai fornitori dell'algoritmo**, ottenendo documentazione sui criteri di selezione e valutazione.

Condurre audit periodici per individuare eventuali distorsioni nei processi decisionali automatizzati.

Introdurre **supervisione umana** nelle decisioni finali di selezione, affinché un recruiter possa correggere eventuali errori dell'IA.

Implementare **test di equità e imparzialità** sull'algoritmo prima della sua effettiva applicazione nel processo di selezione.

COMPLIANCE E RISCHI OPERATIVI

- Definizione delle basi giuridiche per il trattamento dei dati, tra cui consenso, obbligo contrattuale e interesse legittimo.
- **Analisi della necessità dell'IA nei processi decisionali per evitare discriminazioni e garantire la trasparenza.**
- **Limitazione della raccolta di dati sensibili per ridurre i rischi di esposizione e trattamento non conforme.**
- Audit periodico per verifica e cancellazione dei dati non necessari, migliorando la sicurezza e riducendo il rischio di violazioni.

2° ESEMPIO: IA PER LA GESTIONE DELLE PROMOZIONI INTERNE

Un'azienda decide di automatizzare il processo di promozione interna con un sistema di IA, che valuta parametri come performance, produttività e formazione. Tuttavia, un'analisi del DPO rivela che il sistema penalizza sistematicamente i dipendenti che hanno usufruito di congedi parentali o lunghe assenze per malattia.

PROBLEMI INDIVIDUATI:

Discriminazione indiretta: il sistema considera le assenze come fattore negativo, senza valutare il contesto.

Opacità nelle decisioni: i dipendenti non ricevono spiegazioni chiare sui criteri adottati.

Violazione dell'art. 22 GDPR: una decisione completamente automatizzata non dovrebbe avere un impatto significativo sulla carriera del dipendente senza possibilità di revisione umana.

SOLUZIONI OPERATIVE

Escludere i dati sensibili (assenze per malattia o congedi parentali) dall'analisi dell'IA, assicurando che non influiscano sulle decisioni.

Introdurre un processo di revisione umana, affinché un manager possa validare le decisioni proposte dall'algoritmo.

Fornire trasparenza ai dipendenti, spiegando chiaramente i criteri di valutazione adottati.

Effettuare test di impatto sulla non discriminazione prima dell'implementazione del sistema.

Creare un meccanismo di contestazione, permettendo ai dipendenti di segnalare errori o ingiustizie nelle valutazioni.

RACCOLTA DATI NEI PROCESSI DI SELEZIONE

Un'azienda raccoglie CV, referenze e informazioni personali per l'assunzione di uno sviluppatore software. Il DPO nota che alcuni dati richiesti (ad es. informazioni sulla salute) non sono strettamente necessari.

SOLUZIONI OPERATIVE:

Limitare la raccolta ai **dati essenziali per la selezione**, evitando richieste non pertinenti.

Fornire **informazioni chiare ai candidati** sul trattamento dei loro dati personali.

Garantire la **conservazione limitata nel tempo**, cancellando i dati dei candidati non selezionati dopo un periodo definito.

4° ESEMPIO: GESTIONE DI UN RECLAMO PER DISCRIMINAZIONE

Un dipendente presenta un reclamo per discriminazione in ambito lavorativo. Il DPO collabora con HR per raccogliere i dati pertinenti senza violare la riservatezza.

SOLUZIONI OPERATIVE:

Definire procedure chiare per la gestione dei reclami, garantendo equità e trasparenza.

Limitare la raccolta ai **dati strettamente necessari** per l'indagine, evitando accessi non giustificati a informazioni sensibili.

Garantire la protezione dell'identità del segnalante, se richiesto.

FORMAZIONE E GESTIONE DELLE VIOLAZIONI

- Formazione HR su protezione dati e gestione IA per una maggiore consapevolezza dei rischi e delle normative.
- Cultura aziendale della protezione dati , incoraggiando i dipendenti a segnalare problematiche.
- Implementazione di un piano di risposta alle violazioni dei dati con ruoli e procedure definite.
- Notifica all'Autorità Garante entro 72 ore (art. 33 GDPR), includendo dettagli sulla natura della violazione e sulle misure adottate.
- Esempio pratico: violazione dei dati dei candidati e gestione del data breach attraverso audit interno e comunicazione trasparente.

INTERAZIONE TRA DPO E HR

- Il DPO fornisce consulenza strategica a HR su raccolta, conservazione e accesso ai dati personali.
- Linee guida per gestire le assunzioni, minimizzando i dati raccolti e garantendo il rispetto delle normative.
- Valutazioni delle performance trasparenti e non discriminatorie, con metriche oggettive e revisioni periodiche.
- Gestione delle controversie lavorative nel rispetto dei diritti dei dipendenti e delle politiche di protezione dei dati.
- Audit e monitoraggio per garantire la conformità normativa e la protezione delle informazioni aziendali.

GESTIONE DELLE RICHIESTE DEI DIPENDENTI

Diritti fondamentali:

- Diritto di accesso ai dati personali trattati dall'azienda.
- Diritto di rettifica per correggere errori nelle informazioni registrate.
- Diritto alla cancellazione dei dati personali quando non più necessari.

Procedure operative per la gestione delle richieste:

- Canali di comunicazione dedicati per ricevere e rispondere alle richieste.
- Tempistiche definite per la risposta, in linea con il GDPR.
- Formazione del personale HR sulla gestione efficace delle richieste.

RICHIESTA DI ACCESSO, RETTIFICA E CANCELLAZIONE IN UN'AZIENDA IT

Un dipendente di un'azienda di sviluppo software, invia una richiesta all'ufficio HR per conoscere quali dati personali vengono trattati dall'azienda su di lui, in base all'art. 15 del GDPR (Diritto di accesso).

IMPATTO GDPR:

L'azienda ha un mese di tempo per fornire una copia dei dati personali in forma comprensibile e gratuita.

L'HR, in collaborazione con il DPO, raccoglie i dati dal sistema di gestione HR, dalle email aziendali e dai report di valutazione delle performance.

Viene generato un report dettagliato che include:

- Dati anagrafici
- Storico delle valutazioni
- Formazione completata
- Log di accesso ai sistemi aziendali

SOLUZIONI OPERATIVE:

L'azienda fornisce i dati al dipendente in un formato leggibile e gli spiega le finalità del trattamento.

Se alcuni dati sono stati condivisi con terze parti (es. società di formazione), deve essere indicato nell'informativa.

- Il DPO ha un ruolo essenziale nella gestione dei dati personali HR e nella conformità normativa.
- L'IA rappresenta opportunità e sfide: se mal gestita, può generare discriminazioni e violazioni della protezione dati;
- Necessario un equilibrio tra compliance normativa e innovazione tecnologica, con controlli costanti su trasparenza ed equità.
- Promuovere una cultura aziendale etica e responsabile, attraverso formazione continua e audit periodici.
- Il futuro della gestione HR richiede un approccio proattivo, con il DPO come garante della protezione dei dati e della giustizia organizzativa.





CONSILIA BUSINESS MANAGEMENT S.r.l.

• Corso Europa, 13 – 20122 Milano

• **TEL:** +39 02 873 89 370 | **Fax:** +39 02 873 89 371

• **Sito web:** www.consiliabm.com

• **MAIL:** segreteria@consiliabm.com

info@consiliabm.com