

LA GESTIONE DEL CAPITALE UMANO

# lavoro



### Master

I corsi in gestione delle risorse umane proposti da 5 scuole di alta formazione in Europa

Nei box delle competizioni di moto e auto i nuovi meccanici sono ingegneri e tecnici che escono dalle accademie della Motor Valley

— a pagina 27

Trova di più sul sito lavoro.ilssole24ore.com

.professionisti .casa — LUNEDÌ .export — MARTEDÌ .lavoro — MERCOLEDÌ .nòva.tech — GIOVEDÌ .marketing — VENERDÌ .moda — SABATO .lifestyle — DOMENICA



La sfida dei flussi dei dati. Le nuove disposizioni in materia di privacy porteranno a rivedere organigrammi e funzionigrammi delle aziende

**Il regolamento.** In vigore da maggio, il Gdpr sta trasformando la vita in azienda: nuove figure e procedure, dalle paghe alle presenze, ai provvedimenti disciplinari

## Con la nuova privacy al centro le risorse umane

Aldo Bottini  
Paolo Pucci

Entrata in vigore, il 25 maggio scorso, del regolamento europeo sulla protezione dei dati personali (Gdpr) ha segnato una tappa importante nella vita delle aziende italiane. Il regolamento ha impattato su tutta la vita dell'impresa: è una norma che sovrappone e incrocia ambiti diversi, per funzionare, deve tenere conto di tutti. Information technology, vendite, compliance, commerciale, marketing: tutte le funzioni aziendali trattano dati e devono, dal 25 maggio scorso, farlo secondo le indicazioni del regolamento. È quindi legittima, a questo punto, una domanda: quale è la funzione aziendale che si candida a gestire l'incrocio detto sopra? Quale la funzione più adatta a fungere da raccordo tra le altre funzioni in materia di privacy? La risposta dipende da una serie molto ampia di variabili. Tuttavia, non sarebbe sbagliato rispondere: la funzione Hr. Infatti, i responsabili del personale sono tradizionalmente al centro della vita aziendale e, in aggiunta, riforme di impianto e impatto paragonabile al Gdpr hanno trovato in passato negli Hr i gestori ideali, basti pensare alla sicurezza sul lavoro e alle sue procedure, o ai requisiti introdotti dai Jobs act per il controllo a distanza dei dipendenti. Tutte norme che presuppongono una solida struttura di procedure e documenti e un'attenzione costante per organizzazione e dinamiche tra soggetti e uffici. Per valutare questa ipotesi, è utile passare in rassegna le principali novità

introdotta dal regolamento e analizzare i punti di contatto con la funzione di responsabile del personale. In primo luogo il Gdpr impone chiarezza di ruoli e organizzazione: per funzionare correttamente la privacy in azienda necessita di un organigramma e delle relative nomine incarichi; questi nuovi requisiti possono essere gestiti in parallelo a organigrammi e funzionigrammi già in atto. Medesimo discorso, di organizzazione e monitoraggio, si può applicare al registro dei trattamenti della società, il documento che anche la nostra Autorità garante indica come modalità regina per dimostrare il rispetto dei requisiti Gdpr. La funzione di gestione del personale, con la sua conoscenza di ruoli, responsabilità e job description si candida immediatamente alla tenuta e all'aggiornamento del registro stesso, con il ruolo di collettore e custode del medesimo. Ai di là, infatti, dell'opera di adeguamento nell'immediatezza dell'entrata in vigore del provvedimento, il modo di operare prescritto dal regolamento dovrà diventare la modalità automatica (privacy by default) di ogni procedura aziendale. La comunicazione (a tutti i dipendenti) e la formazione (di tutti i soggetti interessati) in materia di corretto trattamento dei dati rientra, o almeno così pare logico pensare, nella più ampia tenuta di registri e attività di formazione già demandata alle risorse umane. A ciò si aggiunge che solo con una gestione centralizzata e precisa dei processi sarà possibile mettere in atto efficaci rimedi in caso di data breach o infrazioni, evitando così le sostanziali e temute sanzioni previste dal Gdpr. Le attività che abbiamo citato finora ora costituiscono aree di intervento

### LA CHECK LIST DEL MANAGER HR

- 1**  
**AUDIT E NOMINE**  
Svolgere un audit in merito ai trattamenti realizzati, alle modalità con cui sono svolti e all'organizzazione interna del dipartimento. Verificare che i soggetti autorizzati siano stati nominati. Definire i compiti nel dipartimento
- 2**  
**DENTRO E FUORI AZIENDA**  
Verificare le garanzie di rispetto della normativa e partecipare alle nomine per i responsabili esterni del trattamento. Verificare le misure di sicurezza adottate e partecipare alla definizione di misure più adeguate
- 3**  
**INFORMATIVE**  
Predispone e inviare le informative per le varie categorie di soggetti interessati (dipendenti, candidati, consulenti, agenti). Partecipare alla stesura del registro dei trattamenti, per quanto di competenza
- 4**  
**POLICY E FORMAZIONE**  
Partecipare alla stesura della privacy policy aziendale. Verificare e occuparsi della formazione del personale in materia di privacy. Essere coinvolto nei team dedicati ai data breach e gestione richieste degli interessati

compatibili ma nuove per i responsabili Hr. Tutti i requisiti visti fin qui, infatti, nascono con il regolamento e costituiscono attività inedite, finora, all'interno delle aziende. Pure inedita è la tenuta dei rapporti con il Dpo, o vesia nominato (non è un obbligo per tutti) sarà utile individuare all'interno dell'azienda un interlocutore abituale, capace di instaurare con lui, o lei, una relazione costante e fruttuosa, per approfittare al meglio dei nuovi strumenti del regolamento. A questo si aggiunge, sin da ora, la gestione dei dati Hr propriamente

detti (paghe, presenze, procedure disciplinari, investigazioni interne) e defettarsi secondo i nuovi requisiti con attenzioni finora sconosciute, chiudendo il cerchio della proceduralizzazione da cui siamo partiti. La centralità del ruolo degli Hr con riferimento ai nuovi obblighi imposti dal Gdpr sembra poi confermata anche da alcune disposizioni del decreto legislativo 101 del 10 agosto 2018, di adeguamento della normativa nazionale al Gdpr stesso, pubblicato sulla Gazzetta ufficiale pochi giorni fa. L'articolo 17 del

decreto, infatti, impone l'applicazione generale (salvo eccezioni) del rito lavoro alle controversie in materia di protezione dei dati. Se è logico pensare che, per le peculiarità del rito e la conoscenza dello stesso, le controversie in questo ambito verranno affidate prevalentemente ad avvocati e giuristi, diventa altrettanto logico e naturale che tal soggetto, necessariamente esterno, venga supportato da chi nelle aziende è abituato a farlo e conosce a sua volta il rito: gli addetti alle risorse umane, appunto. In tal senso, poi, depongono anche le disposizioni del decreto che pongono una particolare attenzione sui trattamenti svolti nell'ambito del rapporto di lavoro: si vedano a tal proposito gli articoli 9 e 21. Il primo prevede la promozione da parte del Garante di regole deontologiche ad hoc per tali trattamenti, con possibilità di individuare anche specifiche modalità per le informazioni da rendere ai lavoratori. Il secondo, poi, cita espressamente l'autorizzazione generale del Garante relativa al trattamento di dati sensibili nell'ambito del rapporto di lavoro tra i provvedimenti di cui lo stesso Garante dovrà, nel corso dei novanta giorni successivi all'entrata in vigore del decreto, individuare ed eventualmente aggiornare le disposizioni compatibili con la nuova normativa. Insomma, è evidente che le nuove disposizioni in materia di privacy (Gdpr e Codice privacy così come modificato dal recente decreto) portano con sé, per chi vorrà coglierla, una sfida per rinnovare il ruolo della funzione Hr nelle aziende, restituendo quella centralità che, forse, altre e passate riforme hanno messo in ombra.

### NUOVE FIGURE

#### DATA PROTECTION OFFICER

## Consiglia e verifica sulle disposizioni



Il data protection officer, reso in italiano con «responsabile protezione dati», è l'unica figura introdotta in maniera obbligatoria dal Gdpr (regolamento Ue 679/2016). Il Dpo accorpia almeno due funzioni complementari. Da un lato consiglia e aggiorna l'azienda sulle disposizioni previste dal Gdpr, dall'altro verifica l'applicazione della legge Ue nell'attività dell'impresa, informando e sensibilizzando i colleghi in materia. In aggiunta può svolgere ruoli di consulenza ed è chiamato a cooperare con le autorità in caso di indagini su (presunte) violazioni al regolamento. Le organizzazioni possono scegliere se assegnare l'incarico a una figura interna o selezionare un professionista sul mercato, purché sia in possesso di tutti i requisiti tecnici del caso. Quali sono le competenze indispensabili? Gabriele Faggioli, amministratore delegato Partners Innovations (società di selezione Dpo), spiega che «occorrono competenze verticali in materia di organizzazione, sicurezza delle informazioni e formazione aziendale», da affiancarsi a una conoscenza dettagliata del regolamento. «Tale mix di competenze - dice Faggioli - è infatti pienamente compatibile con il ruolo di Dpo, al quale è richiesto di occuparsi di tutti gli aspetti che impattano sul trattamento di dati personali nell'ambito dei vari processi aziendali».

— Alb.Ma.

© RIPRODUZIONE RISERVATA

#### CHIEF INFORMATION SECURITY OFFICER

## Protegge dai furti di informazioni private



Il chief information security officer è la figura che si occupa di controllare e programmare la difesa dei dati sensibili in azienda. Un ruolo diventato sempre più decisivo nell'era dell'economia digitale e, soprattutto, dei rischi che incombono in caso di furto di informazioni private: un bacino di dati che si è ampliato di pari passo con il boom di prodotti e servizi online, dalle piattaforme di pagamento mobile agli strumenti di gestione di account da remoto. Non esiste un curriculum unico, ma il background più adeguato è di natura tecnica (dall'ingegneria all'informatica), meglio se integrato da una specializzazione in cybersecurity. Come spiega Elisa Schiavon, marketing manager della piattaforma di recruiting Monster.it, il ruolo va oltre la «sola» mitigazione delle minacce provenienti dalla Rete. «È una figura sempre più strategica nelle imprese, che non si limita alla gestione degli aspetti informativi - dice Schiavon - bensì si occupa anche della strategia che sostiene e arricchisce l'attività di business dell'azienda». Oltre alle competenze di carattere più tecnico, bisogna lavorare sulle capacità di relazione e team management, la gestione dei colleghi. «Sono indispensabili - aggiunge Schiavon - sempre di più soft skills di gestione del team e capacità di visione».

— Alb.Ma.

© RIPRODUZIONE RISERVATA

#### RESPONSABILE TRATTAMENTO DATI

## Cura l'assistenza pratica nella gestione dei dati



Il responsabile trattamento dati è definito dal Gdpr come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». Spesso confuso con il data protection officer, il responsabile trattamento ha il compito di eseguire la gestione delle informazioni sulla sola base delle indicazioni ricevute internamente all'azienda (mentre il Dpo svolge una funzione attiva di verifica e controllo sull'implementazione del regolamento europeo). Secondo la definizione dell'articolo 28 del Gdpr stesso, il responsabile trattamento è chiamato a «strappare i dati personali soltanto su istruzione documentata del titolare del trattamento (un'ulteriore figura che decide come e perché debbano essere utilizzate determinate informazioni, ndr), anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale». In aggiunta, la figura è tenuta a garantire assistenza pratica al titolare del trattamento con misure tecniche e organizzative adeguate e a supportarlo nella verifica sul corretto adempimento degli obblighi legali. La figura è chiamata a rispondere di violazioni del Gdpr solo quando agisce in maniera diversa rispetto alle istruzioni del titolare del trattamento.

— Alb.Ma.

© RIPRODUZIONE RISERVATA