Executive Brief

Cloud, conformità legislativa e necessità di una trasformazione nella gestione delle Risorse Umane a supporto della strategia HCM

Sponsorizzato da: ADP

Duncan Brown Alexandros Stratis
November 2016

RAPPORTO SINTETICO

I dirigenti delle Risorse Umane devono affrontare la sfida posta dagli approcci obsoleti alla gestione e all'elaborazione dei dati sui dipendenti. Questi approcci possono variare notevolmente tra sede centrale e affiliate, a causa di una combinazione di fattori quali l'utilizzo di applicazioni software diverse e di fornitori di servizi in outsourcing terzi, nonché la dispersione geografica di un data center distribuito. Analogamente, l'adozione del cloud aumenta ulteriormente la pressione sulle normative in materia di sicurezza.

Per rispondere a queste sfide, e alla necessità di diventare più strategici agli occhi dell'azienda, i direttori delle Risorse Umane promuovono progetti di trasformazione della gestione delle Risorse Umane e investimenti nelle tecnologie correlate. Un ingrediente essenziale per conseguire i risultati attesi di queste iniziative è la collaborazione con un fornitore di tecnologie per la gestione delle Risorse Umane in grado di garantire l'integrazione di approcci coerenti alla protezione dei dati e alla conformità legislativa come best practice nelle proprie offerte di servizi e software.

Una rapida trasformazione del settore della gestione del Capitale Umano (HCM) sta rivoluzionando il modo in cui viene gestita la forza lavoro. Questa trasformazione si incentra sulla valutazione delle prestazioni basata su progetti, collaborazione e risultati, sull'interazione complessiva con i dipendenti e sul modo in cui questi possono pianificare la propria carriera e il proprio futuro. Il reparto Risorse Umane, che storicamente è stato il custode dei dati sui dipendenti, l'amministratore della formazione e il responsabile dell'elaborazione delle transazioni relative alle risorse umane, si sta trasformando in un partner strategico per la crescita dell'organizzazione.

Una rapida trasformazione nell'ambito HCM sta rivoluzionando il modo in cui viene gestita la forza lavoro.

Un elemento chiave della trasformazione della gestione del Capitale Umano riguarda il rapido superamento di soluzioni proprietarie e processi manuali a favore di soluzioni "tutto compreso" e servizi cloud pubblici. L'adozione di soluzioni cloud ha buone probabilità di migliorare l'esperienza dei clienti, oltre a offrire l'efficienza e la flessibilità tipica delle architetture cloud.

Permangono tuttavia le preoccupazioni relative alla sicurezza. Affidare informazioni sensibili a una terza parte è in ogni caso un passo significativo, ma trasferire i dati dei dipendenti nel cloud, in una località sconosciuta protetta da vaghe garanzie di sicurezza, è una soluzione insufficiente per la maggior parte dei dirigenti delle Risorse Umane. Come possono i datori di lavoro essere certi che i dati dei propri dipendenti siano al sicuro?

La partita sta per diventare molto più seria, sia dal punto di vista degli obblighi che delle conseguenze. Il Regolamento Generale Sulla Protezione Dei Dati (GDPR, General Data Protection Regulation), che entrerà in vigore il 25 maggio 2018, innalza i requisiti per la sicurezza delle attività di elaborazione dei dati personali che sono potenzialmente più a rischio. È importante notare che il GDPR è un Regolamento, non una Direttiva, il che significa che si applicherà allo stesso modo in tutti i 28 Stati membri senza richiedere un'implementazione nelle varie legislazioni nazionali.

In vista del GDPR, le aziende hanno difficoltà a comprendere e rispondere ai cambiamenti normativi in atto. I costi e i rischi della mancata conformità possono essere significativi.

Il cloud, se implementato correttamente, può mitigare i rischi di non conformità al GDPR e alle normative locali sul lavoro. IDC ritiene che molte aziende sceglieranno di esternalizzare l'elaborazione dei dati delle Risorse Umane allo scopo di *ridurre* i propri rischi e obblighi di conformità. Tuttavia, un fornitore di servizi per le Risorse Umane in Outsourcing (HRO) deve offrire un solido piano d'azione, mappe del flusso dei dati, piani per la loro conservazione, robuste piattaforme di sicurezza e programmi per il trasferimento dei dati, il tutto coordinato da un ufficio per la protezione dei dati.

Il cloud, se implementato correttamente, può mitigare i rischi di non conformità al GDPR e alle normative locali sul lavoro.

Questo documento spiega l'impatto del GDPR e mostra come il cloud può facilitare la conformità invece di ostacolarla, migliorando allo stesso tempo la strategia digitale dell'azienda per la gestione del Capitale Umano.

IL MUTAMENTO DELL'AMBIENTE NORMATIVO PER I DATI SULLE RISORSE UMANE

Il GDPR è la modifica delle leggi sulla protezione dei dati più significativa degli ultimi trent'anni. Aggiorna le leggi esistenti, create prima dell'emergere di Facebook, LinkedIn e cloud, e unifica la legislazione sulla protezione dei dati nei 28 Stati membri.

Il GDPR è la modifica delle leggi sulla protezione dei dati più significativa degli ultimi trent'anni.

La Direttiva sulla protezione dei dati esistente risale al 1995, e non è idonea a proteggere i dati personali degli individui in un mondo in cui la conservazione e lo scambio di informazioni personali online sono consuetudini quotidiane. La Direttiva inoltre è stata implementata da ogni Stato membro in base alle proprie convenzioni e abitudini culturali in ambito commerciale, producendo una disparità di regimi di protezione dei dati all'interno dell'Unione. Il GDPR è quindi un notevole passo avanti per l'unificazione e la modernizzazione delle leggi sulla protezione dei dati in Europa.

La definizione di "dati personali" è molto ampia: include tutte le informazioni che identificano o possono identificare un individuo, sia direttamente che indirettamente. Questo include gli identificatori ovvi come nome o numero di identificazione, ma anche dati sull'ubicazione o indirizzi IP, nonché informazioni biometriche e genetiche. Un punto importante è che i dati personali includono quelli relativi ai dipendenti di un'azienda oltre a quelli dei suoi clienti.

L'implicazione principale del GDPR per i dati delle Risorse Umane è forse ovvia, ma vale la pena sottolinearla. Con il GDPR, i dati dei dipendenti acquisiscono gli stessi diritti di quelli dei clienti. Questo significa che gli obblighi dell'azienda in materia di protezione dei dati delle Risorse Umane aumentano, così come è obbligatorio garantire ai dipendenti il diritto ad accedere, aggiornare ed eliminare i propri dati. Le conseguenze di una mancata conformità, inoltre, sono significative (come vedremo più avanti).

Con il GDPR, i dati dei dipendenti acquisiscono gli stessi diritti di quelli dei clienti.

Tuttavia, i reparti Risorse Umane non si limitano solo al rispetto del panorama normativo del GDPR e della privacy dei dati; il numero di norme e leggi specifiche di ogni Paese a cui devono conformarsi le aziende rappresenta da solo una sfida non indifferente. L'HR deve mantenere la conformità in cinque diverse aree: benefit e assicurazione, assunzione, sicurezza e rischi sul lavoro, libri paga e gestione del ciclo di vita dei dipendenti.

Sempre più sovente, le organizzazioni chiedono ai propri reparti Risorse Umane di essere proattivi e affrontare tutta una serie di rischi relativi alle persone nelle cinque aree citate. La sfida è più complessa per le organizzazioni che operano in più giurisdizioni, con affiliate o società capogruppo in località diverse. Ciò che importa in questo contesto è capire che la conformità all'interno delle Risorse Umane deve essere vista come una funzione più ampia di gestione del rischio che contribuisce anche all'avanzamento dei programmi per il Capitale Umano.

Inoltre, la conformità contribuisce a innalzare il ruolo dell'HR da un sistema di elaborazione dei dati con una funzione strategica minima a un partner strategico chiave che può ridurre i costi relativi ai rischi per l'organizzazione e allo stesso tempo aumentare la produttività e il coinvolgimento dei dipendenti.

I requisiti di conformità per i reparti Risorse Umane, che richiedono il monitoraggio e la gestione costante dei parametri, vanno dal libro paga e dai contributi fiscali (il "PAYE system" nel Regno Unito o la "impôt sur le revenu" in Francia, ecc.) alla formazione (orientamento iniziale, identificazione delle frodi, ecc.) e ai requisiti di sviluppo professionale (monitoraggio dei crediti per la formazione professionale o altre metriche utilizzate da associazioni e comitati professionali per ottenere l'affiliazione) o alla due diligence nei processi di assunzione e licenziamento, solo per fare alcuni esempi.

CARATTERISTICHE PRINCIPALI DEL GDPR

Come già detto, la definizione di dati personali del GDPR è molto ampia. Dal punto di vista delle Risorse Umane, tutte le informazioni relative a un dipendente sono protette, e alcune categorie di dati non possono addirittura essere raccolte. Questo include le cosiddette "categorie speciali" di dati, i cosiddetti "dati sensibili". Tali categorie includono i dati genetici, biometrici e medici oltre alle preferenze o all' orientamento sessuale. Tuttavia, un'importante eccezione a questo divieto è l'elaborazione delle informazioni ai fini della medicina preventiva e del lavoro o per la valutazione della capacità lavorativa di un dipendente (GDPR, articolo 9).

Il GDPR introduce inoltre una corresponsabilità tra titolari del trattamento dei dati (tipicamente, nel contesto dei dati delle Risorse Umane, il datore di lavoro) e i responsabili del trattamento dei dati (terze parti che elaborano i dati per conto del datore di lavoro) in determinati casi. Questo è importante per i datori di lavoro che impiegano o intendono impiegare servizi esterni per il trattamento dei dati delle Risorse Umane.

In termini di requisiti di sicurezza, il GDPR rimane deliberatamente vago. Dei 99 articoli del testo finale del GDPR, solo uno (articolo 32) fa specificamente riferimento alle disposizioni sulla

sicurezza, ed è molto poco dettagliato. L'indirizzo generale del Regolamento è che le organizzazioni devono prendere in considerazione la tecnologia più all'avanguardia, oltre al costo, al rischio e al contesto aziendale. Le organizzazioni devono quindi decidere che cosa significa "all'avanguardia" nel proprio contesto: un compito non semplice. L'articolo inoltre incoraggia fortemente, pur senza renderle obbligatorie, la crittografia e la pseudonimizzazione (approssimativamente equivalente alla tokenizzazione).

Si noti tuttavia che la sicurezza è parte integrante dei principi relativi al trattamento dei dati personali (articolo 5). In particolare, il GDPR prescrive che i dati personali siano trattati in modo tale da "garantirne un'adeguata sicurezza". Se dunque il GDPR è impreciso in merito alle misure da adottare per garantire la sicurezza, è molto esplicito sull'importanza della sicurezza.

Il GDPR è impreciso sulle misure da adottare per garantire la sicurezza, ma molto esplicito sull'importanza della sicurezza.

Dal punto di vista della gestione del Capitale Umano, il GDPR indirizza i direttori delle Risorse Umane verso una serie di importanti decisioni tecnologiche. Benché non sia obbligatorio, molti direttori delle Risorse Umane considereranno opportuna la crittografia di tutti i dati dei dipendenti, sia inattivi che in transito e nei backup. Il GDPR rende invece obbligatoria la conservazione dei registri del trattamento dei dati e la capacità di facilitare le verifiche per scopi sia di conformità che di indagine legale.

GDPR: non solo sicurezza

Molti ritengono, a torto, che il GDPR sia essenzialmente una normativa sulla sicurezza dei dati. Benché la sicurezza dei dati, come abbiamo visto, sia un aspetto importante del GDPR, è un errore considerarla la tecnologia fondamentale in questo contesto. Vi sono altri requisiti che coinvolgono una varietà di tecnologie oltre alla sicurezza.

Ad esempio, il requisito di portabilità dei dati (articolo 20) dà diritto all'individuo di richiedere i propri dati personali dal titolare del trattamento, se possibile in formato leggibile da computer, quando il trattamento dei dati è basato sul consenso dell'individuo o su un contratto. Il diritto di cancellazione (spesso detto "diritto all'oblio", articolo 17) consente all'individuo di richiedere a un titolare del trattamento l'eliminazione dei propri dati personali, sia pure in circostanze specifiche e con numerose eccezioni. Inoltre le regole per il consenso, e in particolare la raccolta del consenso dei genitori per i dati dei minori (articolo 8), diventano notevolmente più severe.

Una delle preoccupazioni principali del GDPR, come dimostrato dai sette articoli dedicati all'argomento, è quella dei trasferimenti di dati (articoli 44-50). I trasferimenti di dati comportano lo spostamento dei dati in un cosiddetto Paese terzo, ossia un paese che non è membro della UE. Lo scopo è garantire che i titolari del trattamento proteggano adeguatamente i dati anche se questi vengono trasferiti fuori dalla propria giurisdizione. L'Unione europea ha due meccanismi per limitare questa minaccia: il controllo del trasferimento dei dati fuori dalla UE e una clausola di extraterritorialità che estende l'ambito del GDPR a tutti i dati relativi a una persona che si trova nella UE, indipendentemente dall'ubicazione di tali dati (vedere articolo 3).

I trasferimenti di dati sono importanti nel contesto dei dati delle Risorse Umane quando i datori di lavoro utilizzano servizi basati su cloud o fornitori di servizi per le Risorse Umane in outsourcing. I datori di lavoro sono tenuti per legge a sapere dove risiedono fisicamente i propri dati, e specificamente se sono conservati fuori dalla UE. È del tutto legale esportare i dati fuori dalla UE, ma questo deve avvenire in conformità a uno dei possibili meccanismi di controllo normativo, che includono:

- Trasferimento sulla base di una decisione di adeguatezza: la UE mantiene un elenco di Paesi le cui leggi sulla protezione dei dati sono considerate adeguate (o equivalenti) al

GDPR. L'elenco comprende solo 12 Paesi e, fatto importante per molti datori di lavoro, non include gli Stati Uniti d'America.

- Norme vincolanti d'impresa: si tratta di un impegno ufficiale da parte di un responsabile del trattamento dei dati a implementare un programma di protezione dei dati che garantisca un livello elevato di protezione in conformità al GDPR e che sia stato approvato dalle autorità di protezione dei dati della UE. Si tratta di un impegno non indifferente, che dimostra un'adesione duratura e legalmente vincolante ai principi di privacy della UE.
- Clausole modello standard inserite nei singoli contratti.
- Consenso al trasferimento dei dati fuori dalla UE da parte dei soggetti dei dati stessi.
- Applicazione di un codice di condotta o meccanismo di certificazione approvato. Entrambe queste strutture sono definite nel GDPR, ma non sono ancora state implementate.

L'altro meccanismo principale per effettuare legalmente trasferimenti di dati si applica nei casi in cui esiste un accordo specifico tra la UE e il Paese terzo. Questo approccio viene tipicamente utilizzato quando non è stata concessa una decisione di adeguatezza. L'esempio migliore di questa situazione è Privacy Shield, un accordo bilaterale tra gli USA e l'Unione europea che consente il trasferimento di dati ai responsabili del trattamento che aderiscono ai termini dell'accordo. Tuttavia, è probabile che Privacy Shield sia messo alla prova in sede legale, come è accaduto con il precedente Safe Harbor. IDC ritiene che per le aziende con sede centrale negli USA che desiderino dimostrare un impegno a lungo termine al rispetto dei principi del GDPR sia consigliabile seguire il percorso delle norme vincolanti d'impresa.

Una dimostrazione di grande attualità del regime di trasferimento dei dati è naturalmente la Brexit. Dal punto di vista della legislazione sulla protezione dei dati, la Brexit è praticamente irrilevante, a causa delle regole sul trasferimento dei dati nel GDPR: se un'azienda del Regno Unito desidera condurre affari con un partner nella UE o elaborare dati personali UE, dovrà rispettare le norme sul trasferimento di dati del GDPR. Dato l'attuale volume degli affari tra il Regno Unito e la UE, è probabile che il Regno Unito adotti una legge analoga al GDPR al momento dell'uscita dalla UE, e in effetti l'ICO (ufficio del commissario per l'informazione) ha già dato indicazioni in questo senso.

Dal punto di vista della legislazione sulla protezione dei dati, la Brexit è praticamente irrilevante.

Sanzioni per la mancata conformità

Si è parlato molto delle sanzioni amministrative "effettive, proporzionate e dissuasive" che possono essere imposte dagli enti regolatori. In particolare è stata evidenziata la sanzione massima fino a 20 milioni di euro o il 4% delle entrate annuali globali, se superiore. È da notare che questo livello di sanzioni si applica solo alle violazioni relative ai principi del GDPR (articolo 5), ai diritti fondamentali dei soggetti dei dati come il consenso e la cancellazione e ai trasferimenti di dati. Le violazioni dei dati in sé, derivanti ad esempio da debolezze nella sicurezza, comportano sanzioni di livello inferiore, fino a 10 milioni di euro o il 2% delle entrate annuali globali. I datori di lavoro potrebbero essere più preoccupati dall'obbligo di notificare le violazioni. I titolari del trattamento dei dati sono tenuti a notificare l'autorità di vigilanza competente in caso di violazioni dei dati che presentino "un rischio per i diritti e le libertà delle persone fisiche" (articolo 33). In questi casi devono inoltre comunicare l'evento alle persone coinvolte (articolo 34). Questo potrebbe generare pubblicità negativa, che a sua volta potrebbe danneggiare il marchio e la reputazione.

In ultima istanza, un'autorità di vigilanza ha il potere di ordinare la sospensione del trattamento dei dati (articolo 58). Questo potrebbe significare in effetti un ordine di interrompere le attività o l'elaborazione di un ciclo salariale (buste paga) se il trattamento dei dati in questione fosse alla base di un processo aziendale fondamentale.

Alla luce di queste sanzioni, non sorprende che il GDPR sia oggetto dell'attenzione dei consigli d'amministrazione di aziende in tutta la UE e anche al di fuori, considerando la clausola di extraterritorialità. Tuttavia è importante capire che le sanzioni (incluse quelle finanziarie) saranno probabilmente imposte ove non sia possibile dimostrare gli sforzi compiuti per assicurare la conformità. Il GDPR pone notevole enfasi sulla conformità in materia di prove, che comprende la creazione e il mantenimento di registrazioni del trattamento dei dati. La possibilità di revisione è essenziale, e la capacità di dimostrare la conformità ("responsabilizzazione") è un principio fondamentale di GDPR.

I VANTAGGI DEL CLOUD: PERCHÉ IL CLOUD NON OSTACOLA MA ANZI AIUTA LE OPERAZIONI HR

Essenzialmente, i servizi cloud sono un tipo di outsourcing. Come per qualsiasi iniziativa di esternalizzazione, è necessario svolgere una dovuta diligenza adeguata nei confronti del fornitore dei servizi. Il trattamento dei dati delle Risorse Umane basato su cloud deve quindi essere sottoposto allo stesso livello di due diligence in sede contrattuale.

La differenza nel caso del cloud è data dalla molteplicità delle sedi di elaborazione che comporta. Le aziende devono mettere in pratica la due diligence ponendo domande diverse sul livello dei processi implementati per la sicurezza e la protezione dei dati e analizzando i rapporti delle revisioni, compresi i rapporti di terze parti indipendenti eventualmente resi disponibili dal fornitore dei servizi cloud. Ad esempio, è essenziale comprendere la sicurezza fisica del data center in cui vengono conservati i dati personali. Un fornitore credibile potrà garantire un livello di sicurezza almeno equivalente a quello delle più grandi imprese, e con tutta probabilità migliore di quello del datore di lavoro medio. Questo comprenderà probabilmente la certificazione ISO 27001 e (sempre più) 27018, che riguardano in particolare la sicurezza dei dati personali nei cloud pubblici.

Non esistono impedimenti tecnici all'hosting dei dati delle Risorse Umane nel cloud.

Non esistono quindi impedimenti tecnici all'hosting dei dati delle Risorse Umane nel cloud. Alcune aziende possono optare per una configurazione con un data center situato nella UE che fornisca certificati comprovati di sicurezza fisica e logica. Inoltre, l'accesso ai dati europei deve avvenire solo dall'interno della UE: l'accesso dall'esterno dell'Unione europea costituirebbe un trasferimento di dati (effettuato dai dati in transito), riducendo l'efficacia dei data center con sede nella UE.

La maggior parte delle soluzioni basate su cloud richiederà trasferimenti di dati fuori dalla UE in misura maggiore o minore. I fornitori hanno sviluppato varie soluzioni per proteggere i dati personali, tra cui clausole contrattuali modello. Tuttavia, le norme vincolanti d'impresa sono considerate la forma più robusta di garanzia legale per i trasferimenti di dati.

Le norme vincolanti d'impresa sono considerate la forma più robusta di garanzia legale per i trasferimenti di dati.

Molte aziende sceglieranno di esternalizzare l'elaborazione dei dati delle Risorse Umane allo scopo di ridurre i propri rischi e obblighi di conformità. I datori di lavoro non possono eliminare il rischio, ma scegliere un fornitore credibile è una misura appropriata da adottare.

I FORNITORI DI TECNOLOGIE E IL LORO RUOLO NELLA TRASFORMAZIONE HR E NELLA COMPLIANCE

Si dice spesso che le aziende possono esternalizzare le attività, ma mai la responsabilità. Questo rimane vero nell'ambito del GDPR, ma l'ampliamento della responsabilità a includere i responsabili

del trattamento significa che almeno parte della responsabilità in materia di conformità può essere trasferita a un fornitore di servizi di trattamento dei dati., esterno

Il titolare del trattamento mantiene comunque la responsabilità, e deve essere in grado di dimostrare la conformità, nei riguardi dei principi fondamentali del GDPR (articolo 5); ma il requisito principale di un responsabile del trattamento dei dati è la capacità di implementare le misure tecniche e organizzative concordate con il titolare. Il responsabile è anche soggetto alle stesse sanzioni per la mancata conformità. La domanda che sorge spontanea è quindi questa: come può un titolare del trattamento dei dati stabilire se un responsabile del trattamento sia in grado di soddisfare questo requisito?

Il GDPR definisce a livello legislativo codici di condotta e certificazioni, ma attualmente nessuno di questi due meccanismi esiste all'atto pratico. I responsabili del trattamento possono quindi convincere i datori di lavoro delle proprie credenziali con altri mezzi complementari, come le certificazioni ISO 27001 (gestione della sicurezza delle informazioni), 27018 (protezione dei dati personali nei cloud pubblici) o 29100 (framework per la privacy), rapporti di revisioni indipendenti e norme vincolanti d'impresa, che dimostrino l'impegno organizzativo a lungo termine per l'adesione ai principi del GDPR da parte dei responsabili del trattamento. Le norme vincolanti d'impresa sono considerate lo standard di riferimento per la protezione dei dati dalle autorità competenti in materia della UE.

Con l'approssimarsi della scadenza del 25 maggio 2018, i datori di lavoro non devono trascurare il GDPR e i notevoli cambiamenti che comporterà.

Una sfida per i fornitori di servizi per le risorse umane in outsourcing (HRO) è quella di realizzare efficienze operative nella gestione di più datori di lavoro operando su vasta scala e allo stesso tempo dimostrare la propria conoscenza delle leggi e delle pratiche locali in materia di normative e pratiche del lavoro. Devono quindi essere internazionali dal punto di vista delle operazioni ma locali nell'implementazione: IDC ritiene che pochi fornitori di servizi HRO saranno in grado di assicurare questa combinazione di competenze.

Una considerazione importante per gli specialisti delle Risorse Umane è il fatto che l'azienda moderna, vuole e si aspetta di più dal reparto HR. In passato i sistemi per le Risorse Umane erano sistemi di archivio con un limitato valore strategico aggiunto dal punto di vista dell'organizzazione, e si concentravano esclusivamente sulla gestione degli aspetti più semplici del ciclo di vita professionale dei dipendenti.

Una considerazione importante per gli specialisti delle Risorse Umane è il fatto che l'azienda moderna vuole e si aspetta di più dal reparto HR .

Nel tempo, con l'evoluzione delle capacità, delle normative e soprattutto del ruolo assegnato alle Risorse Umane, gli specialisti del settore aspirano a essere più strategici e offrire più informazioni approfondite e valore all'intera organizzazione. In quest'ottica non è possibile sottovalutare la conformità legislativa: al contrario, la gestione di questo elemento dal punto di vista delle Risorse Umane diventa un fattore di mitigazione del rischio essenziale per l'azienda, con il potenziale di ridurre i costi e proteggere l'azienda dalle controversie legali, nonostante la maggiore complessità e portata del ruolo del reparto Risorse Umane.

RACCOMANDAZIONI CHIAVE

Non trascurate il GDPR

Con l'approssimarsi della scadenza del 25 maggio 2018, è importante che i datori di lavoro non trascurino il GDPR e i notevoli cambiamenti che comporterà. L'ambito legale e tecnico del GDPR è estremamente ampio e la maggior parte delle organizzazioni faticherà a implementare in pieno il

Regolamento entro la data della sua entrata in vigore. Quei datori di lavoro che non abbiano ancora iniziato a esaminare l'impatto del GDPR dovrebbero farlo immediatamente.

Il GDPR è un'opportunità

È facile considerare il GDPR, con tutti i suoi cambiamenti, come un notevole ostacolo da affrontare e una distrazione dalle normali attività aziendali. In realtà, IDC ritiene che il GDPR offra opportunità non trascurabili alle organizzazioni dei datori di lavoro. Crea un ambiente normativo chiaro e uniforme per i trasferimenti di dati che sono alla base dei servizi per le Risorse Umane in outsourcing nel cloud. Con le garanzie di sicurezza appropriate da parte del fornitore, le aziende possono utilizzare questo tipo di outsourcing in modo sicuro e legale nel quadro della propria strategia per la gestione del Capitale Umano.

La conformità è una partnership

Nel mese di agosto 2016, IDC ha completato il suo *Sondaggio Sulla Gestione Del Capitale Umano* in Europa occidentale, con oltre 250 risposte da parte di responsabili decisionali e manager nell'area delle risorse umane. Nel nostro sondaggio, le problematiche relative alla privacy dei dati e ai cambiamenti legislativi (GDPR) sono viste come una preoccupazione centrale da un partecipante su tre, mentre solo il 23% appare poco o per nulla preoccupato. La maggioranza dei partecipanti (76%) considera ancora la privacy dei dati e la conformità (al GDPR e ad altre leggi) tra i fattori che influenzano la decisione di acquisto di una soluzione per la gestione del Capitale Umano.

È essenziale che i fornitori offrano alle divisioni HR le informazioni e gli strumenti necessari, insieme alla garanzia che le soluzioni offerte siano conformi e sicure, poiché possono aiutare i reparti Risorse Umane a raggiungere meglio i propri obiettivi a lungo termine, ossia la trasformazione da una funzione di back-office a un partner di valore per il consiglio di amministrazione.

Informazioni su IDC

IDC (International Data Corporation) è il primo gruppo mondiale specializzato in ricerche di mercato, servizi di consulenza e organizzazione di eventi nei settori dell'Information Technology, delle telecomunicazioni e della tecnologia consumer. IDC aiuta i professionisti IT, i dirigenti aziendali e la community degli investitori a prendere decisioni basate su elementi concreti in merito agli acquisti nel settore della tecnologia e alle strategie di business. Oltre 1.100 analisti di IDC in 110 paesi di tutto il mondo mettono a disposizione la loro esperienza e capacità a livello globale, regionale e locale circa le opportunità e le tendenze della tecnologia e dell'industria. Da 50 anni, IDC fornisce analisi strategiche per aiutare i propri clienti a raggiungere i loro principali obiettivi di business. IDC fa parte del gruppo IDG, società leader a livello mondiale nel settore dell'editoria, della ricerca e degli eventi in ambito tecnologico.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com