PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5138 di Mercoledì 06 aprile 2022

La gestione e la protezione dei dati dei lavoratori in Azienda

Sicurezza, mobilità, compliance ed efficienza sono i nuovi valori della digital transformation per l'HSE Manager

La gestione e la protezione dei dati aziendali è ormai diventata una priorità assoluta nell'attuale contesto della digital transformation, in cui il patrimonio informativo aziendale è composto da dati personali, progetti e proprietà intellettuali, che hanno un valore inestimabile.

L'entrata in vigore del GDPR e la progressiva consapevolezza di dover garantire la sicurezza dei dati impongono alle aziende l'utilizzo di particolari attenzioni su quelli che sono i dati sensibili.

Le modalità di trattamento dei dati personali e la relativa accountability dipendono dall'attività e dalla struttura organizzativa dell'azienda, quindi diventa fondamentale capire sin da subito quali sono i dati personali trattati.

Infatti, oltre a nome e cognome potrebbero essere trattati altri dati personali come il codice fiscale, l'ubicazione, i dati bancari che coincidono tra personale e aziendale, indirizzo mail, ecc...

Dati che per la propria insita natura "sensibile" necessitano di maggiore attenzione e protezione, anche in vista dei possibili rischi connessi alle violazioni digitali, sempre più all'ordine del giorno.

Considerando che, il loro attuale valore per le Aziende è altissimo, tanto da essere considerati "il nuovo petrolio", appare evidente che se si rispettano regole e procedure per la protezione dei dati personali, a beneficiarne sarà la stessa organizzazione.

Rispettare il GDPR non significa però limitarsi a trattare i dati osservando i requisiti normativi, ma piuttosto adottare le misure per gestirli e proteggerli.

Ma quali sono gli interventi che le aziende possono mettere in campo?

- **check up** dell'infrastruttura informatica e rete aziendale
- implementazione di **misure di protezione dei dati (cybersecurity)** attraverso interventi IT interni all'azienda o con l'affidamento a fornitori certificati che offrono adeguati standard in materia
- definizione di **politiche di profilazione**, accessi e permessi sia nella rete aziendale che nell'ambito dei diversi sistemi gestionali, così da evitare l'accesso e/o la modifica di dati da parte di qualunque utente aziendale

- ottimizzazione della **gestione documentale**, tramite la digitalizzazione sicura degli archivi e l'adozione di politiche che definiscono i diversi livelli di riservatezza (pubblico, riservato, ad uso interno) per ciascun documento
- analisi dei diversi **sistemi gestionali implementati in azienda,** al fine di evitare ridondanze, perdita di informazioni e mancato aggiornamento dei dati.

Dunque, appare evidente che per garantire la data security è necessario adottare un approccio strutturato e strategico ed avere la visibilità a 360° di quello che avviene all'interno del proprio perimetro aziendale. Infatti, solo una efficace ed efficiente governance aziendale consente di valutare i rischi informatici associati alla propria realtà, attivando le giuste contromisure per assicurare che gli asset aziendali abbiano sempre dei livelli di sicurezza adeguati.

In linea con queste esigenze di mercato si muove **Wolters Kluwer** che ha realizzato per le Aziende, la soluzione **SIMPLEDO** per la gestione dei **processi HSE** in grado di offrire le migliori garanzie in termini di dati, tecnologia e workflow.



In particolare, **SIMPLEDO**, attraverso la nuova funzionalità **Data Retention**, assicura il rispetto non soltanto del GDPR, che sancisce il diritto di rettificare i dati personali ed alla cancellazione e all'oblio, ma anche l'ottemperanza ad altre normative che impongono alle Aziende di conservare tutte le cartelle sanitarie dei lavoratori, inclusi quelli che hanno cessato il rapporto lavorativo, come previsto nelle seguenti disposizioni:

- **D. Lgs 81/08**
  - Art. 25 (comma 1, lett. e, g, h): conservazione per almeno 10 anni (dalla data di cessazione)
  - Art. 243 (comma 6): conservazione per 40 anni (dalla data di cessazione) per lavoratori esposti ad agenti cancerogeni/mutageni
- **D.Lgs 101/2020**
  - Art. 140 (comma 3): conservazione fino al compimento del 75° anno e almeno per 30 anni dalla data di cessazione del lavoro per lavoratori esposti a radiazioni ionizzanti.

Attraverso la funzionalità **Data Retention**, **SIMPLEDO** consente di anonimizzare ed archiviare tutti i dati dei dipendenti dopo 10 anni dalla data di cessazione del rapporto di lavoro.

L'anonimizzazione consiste nel rendere irriconoscibili i dati del lavoratore (nome, matricola, uo, ...) e nell'archiviare o eliminare i documenti e gli allegati ad esso associati (cartella sanitaria, giudizi di idoneità, ...).

In particolare, il servizio consente di:

- **Individuare** i lavoratori **idonei all'anonimizzazione**
- **Verificarne i dati**, classificandoli correttamente
- **Creare** il **pacchetto di archiviazione** dei dati (da conservare su repository aziendale)

- **Anonimizzare definitivamente** i dati personali dei lavoratori.

Questo processo permette all'Azienda di poter fruire delle informazioni per analisi e ricerche statistiche, senza curarsi di obblighi e responsabilità imposti dalla normativa in materia di protezione dei dati personali.

Ma, nell'ambito della data protection e cyber security, **SIMPLEDO** non si limita a questo.

Infatti, attraverso la funzionalità di **Data & Access Tracing** garantisce la tracciabilità di tutte le attività svolte, la storicizzazione di tutti i dati modificati e/o cancellati ed il monitoraggio puntuale sugli accessi, permettendo di ricondurre le singole azioni di inserimento, modifica e cancellazione dati agli utenti abilitati che le hanno predisposte, nel rispetto dei requisiti previsti dall'art.53 del D.Lgs 81/08.

Inoltre, per assicurare la protezione dei dati a 360°, come anticipato, non si può prescindere dall'adozione di misure volte a proteggere le risorse informatiche ed i dati ospitati. A tali esigenze, **SIMPLEDO** risponde con l'uso della crittografia dei dati sensibili dei lavoratori (encryption at rest and in transit) come quelli sanitari, la gestione sicura di dati/documenti e la gestione delle password GDPR compliant e sicurezza degli accessi (autenticazione a due fattori e/o SSO).

Infine, la piattaforma utilizzata per l'erogazione dei servizi di **SIMPLEDO** è **Microsoft Azure**, il più innovativo e certificato servizio cloud che garantisce massimi livelli di performance, sicurezza e protezione dati, in conformità al GDPR.

Sicurezza, **mobilità**, **compliance** ed **efficienza** sono le **4 parole chiave** che riassumono il valore della **digitalizzazione** per l'**HSE Manager**.

L'attuale gestione dei tuoi processi aziendali HSE è così al sicuro?

Per richiedere gratuitamente una presentazione DEMO, invia una e-mail al seguente indirizzo:
info.simpledo@wolterskluwer.com e/o **compila il form con i tuoi dati.**

Leonarda Cornacchia

HSE Software Marketing Manager

Wolters Kluwer Italia

---

www.puntosicuro.it