IL REGOLAMENTO UE 2016/679: DAL CONSULENTE AL MEDICO COMPENTENTE

Dott.ssa Alessandra BONSIGNORE
Partner assicurativo ANMA

Che il GDPR stia causando non pochi mal di testa non solo alle aziende ma anche ai professionisti non è più una novità.

La normativa introduce un pesante concetto di responsabilità, o meglio di responsabilizzazione: ogni Titolare del Trattamento dei Dati deve selezionare, su una base concreta di competenze, gli eventuali Responsabili del Trattamento dei Dati, i *Data Protection Officer* (DPO) responsabili della protezione dei dati aziendali, e gli eventuali collaboratori interni ed esterni che avranno accesso ai dati personali. Come specificato negli altri articoli pubblicati in questa pagina, il Medico Competente diviene Responsabile del Trattamento dei Dati e di conseguenza ha una dose di responsabilità, in quanto i dati sensibili di cui entra in possesso per esercitare la propria attività sono sotto la sua responsabilità.

Se pensiamo alle realtà aziendali, la responsabilità del dato è direttamente allineata a misure di sicurezza che vengono applicate soprattutto al sistema informatico: password, server, computer dei dipendenti...tutti elementi che devono essere analizzati e strutturati per "proteggere" i dati personali ivi contenuti.

Ma quando si parla di liberi professionisti e nello specifico del nostro caso di Medici del Lavoro, quali sono le azioni accettabili che il singolo può mettere in atto per adeguarsi al GDPR? Sicuramente il fatto di essere titolati come Responsabili del Trattamento pone responsabilità oggettive specifiche. Come possiamo adottare soluzioni a basso costo ma alto impatto in termini di sicurezza, per dormire sonni più tranquilli?

Anzitutto bisogna definire il percorso che compiono i dati cc.dd. particolari.

Da dove arrivano? Come vengono tracciati? Se i dati transitano via posta elettronica è buona prassi proteggere tramite password anche il singolo messaggio di posta, comunicando con altro mezzo tale password. Questo perché le e-mail, e soprattutto i loro allegati, sono qualcosa di estremamente volubile: possono essere scaricati su più *media* e condivisi attraverso altri *media* (ad es. WhatsApp) perdendone così tracciabilità e sicurezza.

Come secondo step, ovvio per molti ma non per tutti, la protezione con password all'accesso di tutti gli strumenti informatici e la dotazione di più profili utente per i dispositivi utilizzati da più persone, onde evitare la condivisione "involontaria" di dati. Per lo *smartphone* la necessità di protezione consente di scongiurare un accesso diretto ai dati da parte di un estraneo in brevissimo tempo.

Per una maggior sicurezza si può pensare di crittografare il disco fisso del *device*. La crittografia è un processo attraverso il quale il contenuto del disco viene "nascosto" da password e così in mancanza di questa il disco rimane illeggibile, inutilizzabile anche su altra macchina. In egual modo lo *smartphone* in mancanza della chiave corretta neppure si avvierà.

Oltre a ciò ovviamente la macchina va protetta con un programma antivirus, o ancora meglio con una suite di protezione completa, in modo da reprimere attacchi e minacce provenienti dal web.

E se siamo abituati ad usare un servizio di *repository*? Questo può essere un problema poiché la normativa sulla privacy obbliga i Titolari del Trattamento ed i Responsabili a comunicare nella informativa dove i dati sono mantenuti e quindi nel caso di servizi come Onedrive o Googledrive o Dropbox inserire l'esatta posizione del server diventerebbe difficile, come sarebbe ugualmente complesso nominare Google o Microsoft Responsabile del Trattamento dei dati. Meglio usare allora piattaforme locali debitamente protette e/o piattaforme *cloud* interamente situate all'interno della Unione Europea ed allineate alla normativa del GDPR.

Infine un accenno alle consuete copie di *backup*: tutti usiamo il sistema per copiare e mantenere copie dei dati o addirittura dell'intero *hard drive*, vale il medesimo discorso fatto poco sopra per password e crittografia, conservando poi in una sede appropriata il disco fisico su cui la copia di *backup* è registrata.