IL REGOLAMENTO UE 2016/679: *UNO SGUARDO DA MEDICO COMPETENTE SULLA PRIVACY*

Dott.ssa Martina BIGOTTI
Medico del Lavoro

Il 25 maggio 2018 entreranno in vigore le nuove norme in materia di *privacy*, relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il Regolamento UE 2016/679 introduce nuove regole in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (c.d. *data breach*); le informazioni relative al Regolamento UE sono reperibili sulla pagina web del Garante della Privacy (in continuo aggiornamento) all'indirizzo http://www.garanteprivacy.it/regolamentoue di cui si raccomanda la consultazione e sulla quale è possibile trovare guide, opuscoli ed un software gratuito per la realizzazione della DPIA – valutazione di impatto sulla protezione dei dati.

Cosa deve fare il Medico Competente per ottemperare agli obblighi di legge in materia ed evitare sanzioni che, pur avendo carattere di effettività, proporzionalità e dissuasività, leveranno il sonno? Come evitare un potenziale danno di immagine, considerato che il garante può Ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali?

Analizziamo per gradi:

a- Non sarà più possibile fare riferimento all'Allegato B: "Disciplinare tecnico in materia di misure minime di sicurezza" che, seppur utile come traccia, contiene misure create circa un ventennio fa e non più adeguate al progresso tecnologico intercorso mentre oggi parliamo di "misure idonee di sicurezza", consultabili sul sito del Garante della Privacy al seguente indirizzo web: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557184

b- Il GDPR introduce una nuova figura: il responsabile della protezione dei dati, a cui dedica la sezione 4 del capo IV del testo. Non sono previsti titoli particolari per la sua designazione, ma questa dev'essere funzionale alle qualità professionali, in particolare la conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché alla capacità di assolvere i compiti di cui all'articolo 39.

Tale Responsabile va designato sistematicamente in 3 condizioni descritte nei seguenti paragrafi: ***a)*** il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; ***b)*** le attività principali del titolare del

trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; *c)* le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

In quell'articolo 9 al punto h) viene ammesso esplicitamente che il trattamento dei dati personali è lecito per finalità di Medicina preventiva o di Medicina del Lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3 così liberando il Medico Competente dall'onere di provare la ragionevolezza della necessità del trattamento di quei dati.

Nei casi diversi da quelli di cui sopra il titolare del trattamento, il titolare del trattamento può o, se previsto dal diritto dell'Unione o degli Stati membri, deve designare tale figura.

Il Medico Competente dovrà partire da una "autoanalisi":

la prima valutazione sostanziale riguarda la protezione fisica ed informativa dei dati: adottare misure di sicurezza per minimizzare i danni in caso di furto o smarrimento dell'hardware con conseguente perdita dei dati o, peggio, furto di dati e credenziali (per esempio tabelle anagrafiche) applicandosi tali misure a tutti i *devices* utilizzati, compreso lo smartphone qualora contenga dati aziendali o venga utilizzato con funzione mail o abbia installate applicazioni integrate.

quindi dovrà essere valutato lo studio medico o i luoghi di lavoro ove il professionista opera: sarà necessario adottare nei gestionali sistemi di pseudonimizzazione e cifratura del dato, che dovrà essere gestito con sistemi di salvataggio quali server, cloud, drive di alta affidabilità: questo adeguamento potrebbe evitare, in caso di eventi negativi, la comunicazione al garante entro le 72 ore (ai sensi dell'articolo 33) perché i dati risulterebbero inutilizzabili da terzi.

in parallelo vi è l'adeguamento formale, che dipende dalla struttura aziendale nella quale il Medico Competente è inserito in regime libero professionale con o senza dipendenti, oppure come Socio di studio polispecialistico o ancora come dipendente di una struttura pubblica o privata che eserciti o meno in regime di convenzione, senza dimenticare le altre figure professionali che vi operano (infermieri, tecnici, personale di segreteria, tecnici di laboratorio analisi integrato allo studio, commercialista , tecnici software e hardware): sarà quindi necessario procedere ad una analisi della propria struttura aziendale: se la struttura risulta articolata e complessa il Medico sarà responsabile

del trattamento per conto del titolare del trattamento, in quanto nominato dal DdL che dovrà inquadrare con adeguata modulistica la sua figura; il Medico titolare della struttura sarà inoltre titolare del trattamento dei dati sensibili e particolari dei dipendenti della struttura.

Entrambe le figure sono disciplinate nel GDPR 679/2016 dal *CAPO IV, Sezione 1, Articolo 24 (Responsabilità del titolare del trattamento) e Articolo 28 (Responsabile del trattamento)*.

I corposi adempimenti formali prevedono contratti scritti, registri dei trattamenti, informative e modulistica di consenso che devono rispondere a requisiti specificati dal GDPR.

Il professionista che utilizza un software, in rete o meno, dovrà verificare che tale programma sia informaticamente adeguato alla normativa e certificato e dovrà nominare per iscritto come amministratore di sistema interno o esterno il manutentore o il perito informatico o la *software house* che di fatto interviene con accesso illimitato e ubiquitario necessario al mantenimento del funzionamento del software stesso.

L'Unione Europea ha indicato la data del 25 maggio non come inizio del percorso di adeguamento, ma come termine ultimo per adeguarsi al GDPR; purtroppo l'Italia non ha al momento un governo in grado di armonizzare il processo di adeguamento. Resteremo in attesa delle norme di transizione per comprendere cosa e quanto della precedente normativa sarà ancora valida dopo il 25 maggio.