PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4503 di Venerdì 05 luglio 2019

Come scegliere un responsabile della protezione dei dati?

Il titolare del trattamento ha una grave responsabilità oggettiva, quando deve selezionare un responsabile per la protezione dei dati: una figura professionale che può aiutare in modo determinante il titolare in fase di trattamento e protezione dei dati.

Nel nuovo regolamento europeo, il responsabile della protezione dei dati, pur essendo un organo di staff, riveste un ruolo determinante nell'assistere il titolare ed il responsabile del trattamento nello svolgere al meglio la loro attività, soprattutto per quanto riguarda la protezione dei dati personali, che essi trattano. Oggi sono presenti sul mercato numerosi soggetti, che dichiarano di avere tutte le competenze necessarie per svolgere questo ruolo, ma altrettanto spesso il titolare del trattamento si trova in dubbio nel valutare queste competenze. Ecco perché ritengo sia opportuno fare il punto della situazione, per mettere i titolari in condizioni di effettuare una scelta, basata su considerazioni oggettive e non su dichiarazioni dei soggetti coinvolti, che meritano di essere attentamente soppesate.

Non v'è alcun dubbio che la professione di responsabile della protezione dei dati rientri fra le attività specifiche, che debbono essere inquadrate, in termini di conoscenza, abilità e competenza in conformità al Quadro Europeo delle Qualifiche (European Qualifications Framework ? EQF), in maniera tale da agevolare i processi di valutazione e convalida dei risultati dell'apprendimento. Detti requisiti sono specificati, a partire dai compiti e dalle attività specifiche, come segue:

- ESPERIENZA- deve esser documentata da dichiarazioni di soggetti terzi, titoli di studio o dichiarazioni del soggetto coinvolto
- ABILITÀ ? deve esser convalidata dal superamento di corsi riconosciuti, impostati e sviluppati secondo lo schema eQF o standard di valore nazionale, europeo o internazionale
- COMPETENZA - deve esser convalidata dal superamento di corsi riconosciuti, impostati e sviluppati secondo lo schema eQF o standard di valore nazionale, europeo o internazionale.

Gli esperti di UNI ed UNINFO hanno lavorato intensamente, con la collaborazione delle strutture coinvolte, nello sviluppare la norma UNI 11697. Questa norma, che definisce i profili professionali relativi al trattamento e alla protezione dei dati personali, è stata messa a punto coerentemente con le definizioni fornite dall'EQF e utilizzando gli strumenti messi a disposizione dalla UNI 11621-1 "Metodologia per la costruzione di profili professionali basati sul sistema e-CF".

A questo punto, è appropriato ricordare il fatto che le norme tecniche sono documenti che definiscono le caratteristiche (dimensionali, prestazionali, ambientali, qualitative, organizzative, di sicurezza...) di un prodotto, servizio, processo o persona secondo lo stato dell'arte. Sempre con l'obiettivo di fare chiarezza, in un contesto piuttosto confuso, vorrei sottolineare che fare norme non significa fare certificazione. La certificazione infatti è la procedura con cui si attesta, mediante verifica da parte di un organo terzo indipendente, che un prodotto, un servizio, un processo o una persona, è conforme ai requisiti specificati.

L'art. 1176 comma 2° del codice civile italiano prescrive che: «Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata»

Per l'art. 2224 c.c. il prestatore d'opera è tenuto a procedere all'esecuzione dell'opera: «secondo le condizioni stabilite dal contratto e a regola d'arte.»

A questo punto, mettiamoci nei panni di un titolare del trattamento che abbia ricevuto un certo numero di proposte di collaborazione, da parte di soggetti, che dichiarano di avere un profilo professionale rispondente alle indicazioni dell'articolo 38 del regolamento europeo, che illustra appunto il profilo del responsabile della protezione dei dati.

Ignoro, per evidenti ragioni, il soggetto che si presenta con una frase del tipo "Dottore, si fidi di me!". È evidente che un approccio del genere è assai poco garantistico ed un titolare, che basasse la sua scelta solo su questa affermazione, potrebbe un domani essere responsabile per aver effettuato una scelta, non è supportata da appropriata diligenza.

Prendiamo in considerazione allora i profili professionali, nei quali il soggetto coinvolto si dichiara di aver partecipato a corsi specifici di formazione.

Un corso di formazione è certamente assai utile, ma il problema da verificare è se i contenuti del corso e la durata del corso sono congrui con la assunzione di sufficienti conoscenze, per poter affermare di essere in grado di svolgere il ruolo di responsabile della protezione dei dati.

Sulla base delle considerazioni che precedono, esiste uno strumento oggettivo, non negoziabile a nessun livello, che conforta il titolare del trattamento nella valutazione di ogni specifica proposta. Lo strumento oggettivo, convalidato dal codice civile, è direttamente connesso al fatto che la durata ed il contenuto del percorso formativo sia conforme a quanto indicato da una norma UNI. Come accennato in precedenza, una norma UNI costituisce stato dell'arte e un soggetto professionale, che operi in conformità a tale norma, opera di conseguenza in un quadro pienamente accettabile.

A questo punto, però, nasce un altro problema: sappiamo benissimo che non è sufficiente aver partecipato ad un corso per aver assorbito tutte le conoscenze che vengono impartite; occorre effettuare una verifica approfondita del livello di assorbimento delle conoscenze e di pratica capacità di utilizzo delle conoscenze stesse. Ecco dove entra in ballo un nuovo strumento garantistico per il titolare, legato alla presenza di una certificazione, rilasciata da ente accreditato, secondo procedure definite dall'ente di accreditamento, cioè Accredia. La presenza di una certificazione, che prevede due esami scritti ed un esame orale, sviluppati da una commissione di competenti valutatori, offre la prova provata al titolare che il soggetto che si presenta dispone, in maniera oggettiva e non soggettiva, dei requisiti necessari per svolgere la funzione che il titolare intende affidargli.

Resta inteso che nulla impedisce che sul mercato siano presenti soggetti che abbiano tutti i requisiti necessari per svolgere la funzione di responsabile a protezione dati personali, ma la mancanza di una certificazione fa sì che la responsabilità della valutazione dei requisiti sia in carico al titolare, con tutti i rischi connessi, soprattutto se il titolare non ha una preparazione sufficiente per valutare tali requisiti. Se invece i requisiti vengono valutati da un ente terzo di certificazione, che opera in un

regime di accreditamento, ed in conformità ad una norma UNI, ci si trova davanti ad una situazione di inoppugnabile idoneità a svolgere la mansione.

Vorrei rammentare ai lettori che queste considerazioni non si applicano solo alla scelta di un responsabile della protezione dati personali, ma anche alla scelta di un collaboratore, di adeguato livello professionale, in molti altri settori. Ecco la ragione per la quale UNI si è dato da fare, con l'umile contributo di chi scrive, per sviluppare norme, per definizione corrispondenti alla regola d'arte, applicabili alla attività di serraturiere, l'attività di fotografo, l'attività di amministratore di condominio e via dicendo. La rispondenza di un profilo professionale ad una norma rappresenta un elemento garantistico in sé, che viene ulteriormente valorizzato, se poi questa rispondenza del profilo professionale è certificata da un ente accreditato.

Spero di essere stato sufficientemente chiaro e che il messaggio sia correttamente recepito da tutti coloro, che per una ragione qualsiasi, debbono scegliere un partner professionale di elevato e confermato livello, per assisterli nella loro attività primaria.

Adalberto Biasiotti

www.puntosicuro.it