Una lacuna che spesso si verifica nelle aziende, è la mancanza di verifiche. Anche se il nostro italico dna, a tratti anche un po' geniale, spesso ci dà una mano nel risolvere i problemi più complessi, è anche vero che gran parte dei disastri accadono proprio per mancanza di controlli periodici adeguati, e sarebbe quindi possibile evitarli se si adottasse un efficace comportamento proattivo.

Quando si parla di infrastrutture informatiche, il pericolo del disastro si percepisce in modo meno lampante rispetto a questioni legate alla sicurezza fisica, eppure non è un caso che il primo illustre Garante della Privacy Stefano Rodotà, abbia affermato che "i dati personali degli oltre 500 milioni di abitanti dei 28 Paesi dell'Unione Europea nel 2020 avranno un valore commerciale stimato attorno ai 1.000 miliardi di euro", l'8% del Pil europeo. Una vera miniera d'oro.

Badando più alla sostanza che ai formalismi, nel testo del nuovo regolamento europeo che attende ormai di essere approvato a breve, il ruolo del responsabile della protezione dei dati (il privacy officer) è presentato come una figura proattiva, con compiti di responsabilità sul sistema di gestione dei dati aziendale, per prevenire o comunque ridurre al minimo il rischio di violazioni, e quindi di potenziali sanzioni, danni, e pericoli di risarcimenti.

Riguardo a questo, è infatti degno di nota che ai sensi delle previsioni dell'art.37 della proposta di regolamento, il privacy officer non deve essere solo un esperto giuridico della normativa, ma ha anche il ruolo di "controllore", avendo l'onere di "sorvegliare l'attuazione e l'applicazione delle politiche in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi".

Per chi non avesse tanta dimestichezza con i sistemi di gestione, l'audit, consiste in una valutazione indipendente che si svolge periodicamente sulla base di un campionamento volta a ottenere evidenze, relativamente ad un determinato oggetto (l'azienda), e valutarle con obiettività, al fine di stabilire in quale misura i criteri prefissati siano stati soddisfatti o meno. Il

concetto di audit può essere applicato a molte attività, comprese quelle della gestione dei dati, come è previsto dallo stesso Regolamento Europeo. L'auditor (il valutatore) è invece la persona che ha caratteristiche personali dimostrate e la competenza per effettuare un audit, nel nostro caso, dovrà essere quindi un esperto di data protection sia a livello giuridico che informatico.

Se è il Privacy Officer a svolgere il ruolo di auditor, egli deve essere oggettivo, imparziale e, soprattutto, non deve avere conflitti di ruolo con l'oggetto dell'audit. In pratica, non deve avere responsabilità dirette con l'organizzazione o con il reparto/ufficio valutati. Una caratteristica dell'auditor spesso trascurata è la spiccata capacità comunicativa, di gestione delle risorse umane centrata sull'assertività, nonché l'abilità di persuadere grazie alla condivisione più che al mero e burocratico richiamo a prescrizioni e regolamenti.

Come negli altri ambiti, anche nel sistema di gestione privacy aziendale, un audit deve avere sempre fissato un obiettivo, che può essere per esempio:

• verificare il grado di conformità alla normativa vigente. Attualmente è ancora il Dlgs 196/2003 insieme ai provvedimenti del Garante, ma prossimamente le regole da rispettare saranno quelle dettate dal Regolamento Privacy UE;

• verificare il grado di conformità alle privacy policy aziendali, ovvero i regolamenti privacy interni dettati dal titolare del trattamento, che tutti i dipendenti sono tenuti ad osservare. Questo richiama l'attenzione sulla necessità che il Privacy Officer abbia ulteriormente competenze in ambito di compliance aziendale;

• qualificare un fornitore di servizi che implichino la gestione e/o il trattamento di dati, (es. un call center in outsourcing, o semplicemente il consulente del lavoro o il CED che elabora le buste paga), per verificare che questo soddisfi la normativa privacy e le nostre privacy policy aziendali, al fine di utilizzarlo successivamente come fonte di approvvigionamento;

• accertare l'efficacia di azioni correttive intraprese a seguito di "non conformità" scaturite da un precedente audit di verifica;

Da non trascurare che, i risultati e l'esito complessivo dell'audit (conclusioni) deve essere documentato attraverso un audit report. Eventuali anomalie (non conformità, punti deboli, difetti, raccomandazioni, ecc) devono essere dettagliatamente precisate. Il report deve contenere o richiamare le modalità per correggere le anomalie. Il rapporto (o relazione di audit) deve essere spiegato e consegnato all'ufficio o reparto auditato, affinchè possa attivarsi per risolvere le non conformità rilevate con le opportune azioni correttive.

In pratica, il privacy auditor è il medico della situazione, l'azienda auditata è il paziente, e il rapporto di audit è la diagnosi con l'eventuale ricetta contenente i medicinali da prendere per guarire se è stato appurato uno stato di malattia.

Certo, a tirare le somme, le competenze richieste al Privacy Officer sono davvero molteplici e complesse. Come se non fosse bastato che questa figura avesse dovuto conoscere bene la normativa sulla protezione dei dati, e possedere skills informatiche, adesso il fatto di dover conoscere anche i sistemi di gestione basati sulle norme ISO e gestire le attività di audit, può sembrare davvero troppo. Ma è l'Europa a chiederlo, e soprattutto è il valore che hanno assunto i dati nei nuovi scenari mondali, che identificano i dati come un vero e proprio "asset" aziendale.

D'altra parte, i privacy officer oltreoceano sono professionisti specializzati altamente preparati, nonchè pagati profumatamente, e per chi possiede già una parte degli skills necessari, può valere la pena adoperarsi per completare il proprio profilo per poter fruire delle opportunità interessanti nel mondo delle nuove professioni che vivono un trend positivo, come quelle dei privacy professionals, specialmente adesso con l'approssimarsi della nuova normativa sulla protezione dei dati taragata UE.

Con competenze così variegate, un bel contributo per fissare i paletti e stabilire quali debbano essere le best practices del modus operandi del Privacy Officer, come la gestione degli audit in tema di privacy, potrà venire dal fronte della normazione volontaria, e per questo Federprivacy insieme a diversi stakeholders del mercato si sono attivati da tempo per pubblicare una norma nazionale sulla figura professionale del privacy officer.

Che sia una legge o meno a imporla, la previsione di un privacy officer nell'organigramma aziendale può solamente essere quantomeno opportuna e giovare a una impresa che decide di designarlo.

Ecco perchè un’azienda il cui core business gira intorno ai dati non può trascurare di sottoporsi a un check-up periodico per verificare il proprio stato di salute attraverso un processo di audit. Inutile dire che, se teniamo alla nostra salute, è fondamentale rivolgersi a un buon medico, adeguatamente preparato, e non al primo che capita solo per sentirsi dire che scoppiamo di salute.