La nuova normativa Europea sulla Privacy (GDPR) e la pericolosità dell'adeguamento apparente

Date : 1 febbraio 2018

Molti di voi saranno già ampiamente al corrente della prossima attuazione, a partire dall'imminente 25 maggio, della nuova normativa europea (EU 679/2016) detta GDPR, di cui si discute ormai quasi quotidianamente nei social media professionali e su riviste specializzate e, sempre più di frequente, su media generalisti.

Da tempo svolgo GDPR audits e progetti di adeguamento alla normativa in contesti, sia nazionali sia internazionali, ed ho avuto modo di valutare diversi modelli e proposte di vario genere per la realizzazione degli adeguamenti, da parte di diverse categorie di protagonisti del settore, ed ho partecipato in prima persona a numerosi progetti di adeguamento al GDPR, avendone anche potuto verificare spesso sul campo la reale effettività.

Molte al giorno d'oggi sono le alternative disponibili sul mercato per aiutare le aziende a valutare il proprio livello di compliance, ad identificare gli adeguamenti da farsi ed a supportarne la realizzazione, sia tramite tradizionali vendor di sicurezza informatica, sia da parte di vari studi legali, sia da società di consulenza specializzate.

A volte le competenze di GDPR dei vari fornitori che si propongono, non sono sempre all'altezza, ma dato l'elevato numero di richieste di progetti GDPR, e lo scarso numero di risorse competenti disponibili sul mercato, è sempre molto difficile, anche all'interno di aziende di nome, trovare personale qualificato.

Le aziende tendono a sottovalutare il problema della fornitura di servizi GDPR, non preoccupandosi abbastanza di dotare gli uffici acquisti di adeguate competenze per capire quali siano i requisiti necessari per le valutazioni dei fornitori di servizi GDPR e, tra i vari requisiti, come dare la giusta importanza ai requisiti veramente importanti rispetto a quelli solo marginalmente utili.

Questo non facilita le aziende a fare le scelte migliori per aiutarle verso il percorso di adeguamento più adatto alle reali necessità della propria organizzazione, così a volte, nelle attività di adeguamento, vengono inseriti requisiti che poco hanno a che vedere con la compliance, o viene data molta importanza a requisiti marginali, con l'effetto pratico di una

riduzione della qualità dei risultati attesi che si traduce in un rischio maggiore per l'azienda, della quale purtroppo, non si rende neppure conto.

Non può essere percepito, perché le aziende mancano spesso di strumenti adeguati, report e KPI misurabili per fare questo tipo di valutazioni, e quindi sono costrette a procedere nelle scelte sulla base di valutazioni estemporanee.

Ad ogni modo, a parziale discolpa delle aziende, è sorprendentemente alto il numero e la tipologia di proposte per l'adeguamento al GDPR, con approcci anche molto diversi tra loro, disponibili sul mercato a prezzi diversi e con risultati anche molto differenti tra di loro.

Il mix di competenze richiesto per il GDPR è veramente elevato ed è difficile trovare skills ed expertise per coprire contemporaneamente molti aspetti diversi tra di loro, come gli aspetti legali, quelli IT, quelli di sicurezza, quelli organizzativi, quelli di processo, quelli di gestione dei fornitori, e a numerosi altri.

Quale sia la soluzione migliore per l'adeguamento alla normativa, dipende ovviamente dalla tipologia di organizzazione e dal livello di complessità della stessa e del contesto in cui opera.

Una volta scelto il proprio fornitore, le aziende poi si ritrovano a seguire dei meccanismi di adeguamento che sono comunque molto simili tra di loro e che si possono sintetizzare nei seguenti passi principali:

1. Un Assessment che mappi l'attuale situazione dell'Azienda rispetto alla compliance, generando la classica GAP Analysis. La Gap Analysis genera una lista di attività, modifiche di processo e dei sistemi, che deve essere implementata in tutta l'organizzazione per arrivare a raggiungere la compliance;
2. Una fase di preparazione e pianificazione, che generalmente consiste nella predisposizione di più progetti separati e da eseguire in parallelo attraverso tutti i dipartimenti dell'organizzazione, nessuno escluso, e nelle varie sedi;
3. Una fase di adeguamento, che prevede la realizzazione dei progetti precedentemente predisposti;
4. Una fase finale di verifica (per la verità non sempre realizzata).

Quello che tipicamente succede è che una volta che la fase di GAP Analisys abbia identificato una serie di punti su cui intervenire all'interno dei vari dipartimenti aziendali, l'azienda si predispone per le attività di adeguamento.

Successivamente partono i diversi progetti di adeguamento per tutte le varie aree aziendali, dal Marketing, all'Ufficio Personale, ai sistemi IT, alla sicurezza di infrastruttura e dei sistemi informativi, al Customer Care, e così via.

Da quel momento in poi, data la complessità dell'attività e l'elevato numero di progetti e personale coinvolto, l'attività più critica, diventa non l'esecuzione dei progetti stessi, ma il loro coordinamento e controllo.

Di solito, si ha più l'impressione che per tutta la durata dei vari progetti di adeguamento, ognuno di essi prende una strada propria, autonoma, avendo come finalità principale quella di implementare i propri obiettivi di adeguamento.

La cosa che sorprende, è che raramente si vedono attività di coordinamento e controllo dei vari progetti in sincronizzazione con il target atteso, che è quello della compliance, mentre invece i programmi di adeguamento sono gestiti in maniera totalmente tradizionale, monitorando semplicemente le attività, i tempi e la conclusione dei progetti.

Il Focus, passa quindi, durante la fase di adeguamento, dalla compliance GDPR alla verifica pura e semplice dell'esecuzione del progetto.

In questo modo, il Management rischia di perdere la visibilità su quello che è, o dovrebbe essere, il vero obiettivo delle attività, che non è quello di portare a termine le attività di adeguamento, ma sostanzialmente di migliorare il livello di compliance GDPR dell'intera organizzazione.

Si dà in effetti per scontato, non si capisce bene sulla base di quali presupposti, che i progetti debbano terminare tutti positivamente e debbano essere realizzati in maniera completa, ottenendo così il risultato tanto desiderato della compliance.

Quindi si presuppone, a mio avviso abbastanza irragionevolmente, che se i progetti di adeguamento sono terminati, il livello di compliance sia automaticamente raggiunto, anche se purtroppo, questo non sempre si rivela essere vero.

Ritengo questo atteggiamento un po' superficiale ed anche potenzialmente pericoloso, dato che chi conosce bene la realtà di adeguamento di sistemi ed organizzazione complesse, sa bene che le cose non vanno sempre esattamente come pianificate.

Durante i vari percorsi di implementazione degli adeguamenti al GDPR, vi sono sempre numerosi ostacoli, come le risorse, il budget, gli imprevisti, o anche situazioni che sulla carta apparivano in un modo che poi si ritrovano ad essere diverse da quello che ci si attendeva in fase di pianificazione, e così via.

Vi sono poi, anche durante le attività di adeguamento, difficoltà dovute magari all'interpretazione della normativa in alcuni contesti di utilizzo per cui la strada scelta potrebbe dover essere rivista in corso d'opera.

Per questo motivo le aziende dovrebbero fare maggiore attenzione alla fase d'implementazione e realizzare metriche e report per misurare KPI specifici sulla compliance in maniera più puntuale rispetto a quanto fanno sinora.

Non solo si rischia, quindi, di non raggiungere il livello di compliance GDPR desiderato, ma si rischia anche di dare vita a quello che io chiamo "adeguamento apparente", dato che in questi casi ci potrà essere anche un miglioramento della compliance GDPR relativo alle evidenze formali, senza che questo debba necessariamente corrispondere ad una vera compliance

GDPR sostanziale .

Alla fine del percorso di adeguamento, il Management delle aziende potrebbe quindi ritrovarsi, nonostante il budget speso e l’impiego massiccio di risorse aziendali, ad avere trascurato problemi non evidenziati.

Le cose potrebbero essere risolte facilmente con un approccio diverso e strumenti adeguati, di cui le aziende dovrebbero dotarsi.

A cura di: **Francesco Falcone**