GDPR – Dove siamo arrivati e quali prospettive ci attendono

Author : Francesco Falcone

Date : 1 ottobre 2018

In molti hanno lavorato a lungo a fianco dei loro clienti e collaboratori, avendo avuto ben chiaro un obiettivo preciso, quello della linea di demarcazione posto dalla data di applicazione della normativa GDPR (EU 679/2016), il 25 Maggio 2018.

Trascorsi ormai diversi mesi da questa data, vediamo, in breve, come le aziende si siano organizzate e quale sia la situazione attuale.

Corporate, grandi aziende e multinazionali

Per quanto riguarda le aziende di grandi dimensioni e quelle che operano in contesti multinazionali, una parte di esse ha già raggiunto un livello di conformità alla normativa che ritiene adeguato, in base agli obiettivi che si è posta.

Molte altre aziende invece, sanno benissimo di non avere raggiunto un livello di compliance sufficiente in ogni area della organizzativa, essendosi concentrate prevalentemente sulle applicazioni ad alto rischio, ed avendo tralasciato il resto.

Queste aziende tipicamente si pongono l'obiettivo di colmare i propri GAPs in termini di compliance, entro la fine di quest'anno, o ai primi del 2019, accettando i rischi residuali riguardanti le proprie mancanze di conformità, ritenendoli sostanzialmente limitati.

Questo atteggiamento, purtroppo, è stato anche parzialmente amplificato dai media, che hanno diffuso spesso e volentieri voci (inconsistenti) sulla "applicazione soft" delle sanzioni nel primo periodo dopo l'entrata in vigore della legge, se non addirittura l'esistenza di un consistente "grace period", cioè di un periodo senza alcuna sanzione.

Piccole e medie aziende

Per quanto riguarda le aziende piccole e medie, è difficile sostenere che gli adeguamenti alla

normativa GDPR siano stati la loro priorità, e molte di esse hanno deciso di rinviare l'attività di adeguamento almeno all'autunno, se non addirittura oltre.

Un po' perché oberati da impegni e scadenze pressanti, connesse alla natura della loro attività, un po' per la mancanza di budget e soprattutto nell'incertezza sull'effettività dell'applicazione della legge.

Da notare che in molti si sono lamentati della confusione generata dalle numerose e variegate proposte di adeguamento a GDPR ricevute, spesso a costi diversissimi tra loro.

Comprensibile. Sarebbe stato difficile per chiunque, e tanto più per aziende senza skills interni adeguati, e senza un supporto specialistico esterno, percepire la differenza tra le varie proposte, alcune magari a prezzo stracciato da consulenti esterni improvvisati, altre da parte di fornitori tradizionali IT e Security (talvolta altrettanto improvvisati) da quelle di società e professionisti specializzati.

Per questo motivo, purtroppo, gli adeguamenti si sono spesso trasformati in una gara al ribasso tra fornitori "GDPR". La necessità di impiegare meno tempo sul cliente e potere quindi abbassare il prezzo di offerta, ha certamente contribuito a rendere più superficiali e meno efficaci i progetti di adeguamento, ed ad aumentare il livello generale di rischio sulla Privacy.

Dove siamo arrivati

Il clamore di cui ha vissuto la fase implementativa, prima del 25 Maggio, oggi si è oramai molto attenuato, per svariati motivi.

Un po' perché l'onda emozionale iniziale, spinta da una scadenza chiara e non rimandabile, e sollecitata da forti pressioni dei media e dei venditori di servizi, che hanno pesantemente utilizzato lo spauracchio delle sanzioni per motivare i clienti e spingere le vendite dei propri prodotti di Security e di consulenza GDPR, al momento si è molto attenuata.

Coloro che hanno realizzato seriamente i propri adeguamenti, spesso esausti dall'enorme impegno profuso nella messa in opera degli adeguamenti tecnici, nelle nuove misure si sicurezza e nella rivisitazione di numerosi processi aziendali, tendono per lo più a tirare il fiato, e a dedicarsi ad attività di rifinitura degli obiettivi raggiunti, consci però di non essere giunti alla fine del lavoro sapendo bene che la conformità deve anche essere mantenuta nel tempo.

Altri, quelli che hanno realizzato i propri progetti a livello più formale che sostanziale, e neppure in maniera completa, sembrano essere arrivati alla fine del loro percorso, e si accontentano di poter presentare delle evidenze formali che ritengono sufficienti per convincere le Authority della loro conformità.

Gli ultimi, infine, ancora attendono guardinghi per decidere quale sarà il momento migliore per fare qualcosa di concreto investendo il minimo del budget possibile. In fondo, come spesso si sente ripetere, prima o poi dovranno pure fare qualcosa per poter dichiarare di essere in regola, almeno da un punto di vista formale.

Quali prospettive

Un recente sondaggio di TrustArc (**fonte : TrustArc GDPR Compliance Status Report @2018)** realizzato intervistando il management delle proprie aziende clienti di ogni fascia ed a livello internazionale, rivela che solo per il 20% la maggior parte dei Manager, ritiene di essere compliant a GDPR, mentre per il 53% ritiene che lo sarà entro fine del 2018, ed il 27% non ha ancora cominciato un percorso di adeguamento a GDPR. Nella sola Europa le percentuali sono un po' migliori, con il 27% che ritiene di essere compliant, il 74% ritiene che lo sarà entro fine 2018 ed il 93% entro la fine del 2019 .

Si ricorda qui che le aziende intervistate avendo già acquisito soluzioni e servizi orientate alla Privacy, rappresentano un sottoinsieme anche qualificato, ma che non rappresenta l'intera categoria, per cui si ritiene che le percentuali complessive siano inferiori, soprattutto nei segmenti medio bassi, che tradizionalmente meno investono nella protezione della Privacy.

Sempre la stessa fonte, riporta che i maggiori problemi siano dovuti alla complessità della legge ed alla difficoltà di reperimento di skills adeguati sul mercato.

Inoltre, una parte consistente degli stessi Manager intervistati, avendo implementato progetti legati alla Privacy ha acquisito consapevolezza sulle "best practice" che dovrebbero essere adottate, ritiene evidente che per loro il raggiungimento di un livello, a loro giudizio, soddisfacente, non sarà il punto finale delle attività, ma che il mantenimento della compliance GDPR richiederà ulteriori budget.

Tanto è vero che il 67% degli intervistati, ha dichiarato che manterrà, se non aumenterà, il budget a disposizione per le attività GDPR anche per il 2019.

Per le piccole medie, tranne le più sensibili, e quelle più esposte sul fronte dei consumatori, vale quanto sopra esposto, per lo più rimangono in attesa del momento migliore per eseguire l'adeguamento.

Anche se esiste per loro un forte pressione da parte delle aziende loro clienti, che hanno bisogno di avere fornitori "compliant a GDPR", molti adottano solo il minimo dei requisiti possibile, e comunque si rivelano disposti a firmare pesanti condizioni capestro con i loro committenti, dichiarando una compliance formale che spesso non sono in grado di dimostrare.

Viene da domandarsi se le aziende committenti, si rendano ben conto del rischio cui si espongono, affidandosi a fornitori che sono conformi a GDPR solo sulla carta.

Nel frattempo, come rilevato dalle varie Authority della Privacy Europee, avviene un diffuso e notevole aumento delle segnalazioni di Data Breach un po' in tutti i Paesi dell'Eurozona.

Dai dati forniti dalle varie Authority, l'incremento del numero delle segnalazioni rispetto all'anno precedente, in cui non era in vigore la GDPR, è generalizzato e generalmente consta di almeno due cifre, se non addirittura di tre, con incrementi che vanno dal 50% in Francia a punte del 500% in Italia rispetto all'anno precedente. *(DPA Francese +56% ; DPA UK : +260% ; Garante*

Privacy : +500%)

Al punto che l’Authority inglese segnala addirittura un “overreporting” con 500 chiamate per segnalazioni di vario genere relative a problematiche sulla Privacy, per ogni settimana.

E’ logico presumere che i nuovi obblighi di segnalazione alle Authority, faranno emergere gradualmente, ma in maniera consistente, una serie di problematiche che precedentemente venivano gestite “in casa” e non comunicate a nessuno, tanto meno agli utenti che ne erano vittime.

In conclusione

Per quanto nei media l’argomento GDPR abbia preso durante l’estate una pausa di riflessione, a partire da Settembre, con la piena ripresa delle attività, l’argomento sembra nuovamente tornato all'attenzione di tutti. Complice anche la pubblicazione della nuova normativa Italiana per l’armonizzazione della vecchia legge sulla privacy a GDPR, entrata in vigore il 19 Settembre .

Inoltre, man mano che aumenterà la consapevolezza dei cittadini sui propri nuovi diritti, o anche se il richiamo alla GDPR verrà visto come un mezzo per vendicarsi di torti, a loro avviso subìti dalle aziende, aumenteranno ulteriormente e proporzionalmente anche i “claims”, cioè le segnalazioni alle Authority.

In realtà, anche se nessuno lo dice espressamente, molti tra gli addetti ai lavori sono in attesa di vedere le prime applicazioni di sanzioni “pesanti “ da parte delle Authority, con la convinzione che ciò darà un segnale forte, e potrà scatenare una nuova corsa da parte delle aziende alla verifica sulla qualità dei propri adeguamenti.

Esattamente il contrario di quanto una corretta gestione della Privacy dovrebbe fare: monitorare la qualità dei risultati di adeguamento, indipendentemente da fattori esterni e dalle sanzioni, con l’ottica di avvantaggiarsi rispetto a quelli che sono ancora lontani dalla conformità.

Purtroppo sembrano ancora essere una rarità le aziende che vedono la GDPR come un opportunità ed un vantaggio nei confronti dei propri concorrenti, invece che come un problema.

Articolo a cura di **Francesco Falcone**