

GDPR: quanto costa la consulenza per adeguarsi ?

dott. Valentino Spataro

Consulente privacy e sviluppatore

@2018 IusOnDemand srl

PrivacyKIT.it

email:

tel:

[Versione audio mp3](#)

Partecipo ad un interessante gruppo su Facebook che parla di GDPR.

Tra i tanti intervento leggo di un organizzatore di manifestazioni al quale sono stati chiesti dai 4.000 agli 8.000 euro da studi legali che alla parola GDPR non sapevano cosa rispondere.

Non credo sia qualcosa di generalizzato ma mi e' sorto subito l'istinto di scrivere un post in materia.

QUANTO COSTA FORMARSI ?

Il GDPR richiede competenze informatiche, giuridiche e esperienza.

Il motivo e' semplice: i provvedimenti concreti interpretano la normativa in modo piu' restrittivo, e a volte espressioni del codice privacy sembrano piu' neutre che nell'applicazione pratica.

I protocolli seguiti dalla Gdp e dal Garante sono quindi un po' piu' complessi, ma non impossibili.

Quindi, per rispondere: ci vogliono settimane di studio per farsi una idea generale, poi altri mesi per capire volta per volta come funziona.

Il tutto aggiungendo una conoscenza dell'informatica, il piu' delle volte.

COSA DEVE FARE IL CONSULENTE ?

Avvocato, giurista, esperto di sicurezza, società di consulenza, giurista d'impresa: tutti possono occuparsene.

Daranno dei documenti, delle guide, delle spiegazioni.

Se richiedi daranno anche i documenti da utilizzare: o modelli adattati o testi realizzati su misura.

BASTA IL CONSULENTE ?

La comprensione di questi documenti e' fondamentale perche' andranno sempre piu' aggiornati, e bisogna capire a cosa servono e come farli.

Valeva per il consulente ex codice privacy, vale ancora di piu' oggi con il GDPR che richiede (di fatto)un registro aggiornato spesso delle attivita' di trattamento.

Quindi il consulente e' quello che risolve la complessità e coinvolge il titolare dei dati perche' possa adempiere.

COSA DEVE FARE IL TITOLARE ?

Come dicevo sopra, deve continuare ad aggiornare i documenti e verificare che si faccia quello che c'e' scritto.

Prassi diverse dalle procedure prefissate non fanno bene al titolare che oggi, piu' di prima, sara' considerato responsabile.

Per risparmiare il titolare dovrebbe censire le proprie risorse autonomamente, da subito, indicando:

- risorse informatiche
- risorse umane
- risorse di dati Completato questo lavoro, il piu' e' fatto.

QUANTO PUO' COSTARE UNA CONSULENZA DI ADEGUAMENTO

Tutti parlano di piccoli adempimenti. In realta' non e' un problema di adempimenti quanto di studio dell'attivita' svolta dal titolare.

Il censimento delle risorse informatiche e' la parte piu' costosa.

L'individuare le soluzioni richiede invece molte conoscenze, sconosciute ai titolari.

L'ideale sarebbe prevedere un servizio di consulenza on demand o a forfait, una prepagata per chiedere ulteriori spiegazioni in ogni momento.

QUALI BUDGET ?

Quelli che i titolari vorrebbero spendere oggi sono (sulla base della mia esperienza):

- da 100 euro per prendere dei pezzi di carta da mettere in faldoni e dimenticarsi tutto
- da 250 euro per chi vuole sapere di piu' e adeguarsi facendo tutto il lavoro successivo da solo
- da 450 euro per chi vuole essere sicuro e coinvolto in una soluzione adeguata per il proprio sito
- da 1500 euro per una attività di censimento in sede
- oltre per attività che trattano dati particolari (ex sensibili) e pericolosi.

COSA MANCA

Non esistono soluzioni informatiche che possano fare tutto il lavoro autonomamente.

Anche le autorità di controllo ne hanno sviluppati, ma si scontrano con la necessità di dover prevedere ipotesi di alta complessità.

Mancano i codici di condotta che le autorità non hanno preparato, lasciando sole le pmi.

Non mancano invece coloro che dicono che conformarsi in tutto è impossibile.

LA SOLUZIONE

La soluzione non è chiudere gli occhi, aspettare che passi, copiare qualcosa da altri, e stare a vedere.

La soluzione è iniziare a tenere un registro dei trattamenti, anche un foglio di word, di excel.

Basta iniziare a descrivere ogni strumento e risorsa aziendale usati per trattare dati personali per rendersi conto di quanto si sia sottovalutato l'importanza degli stessi.

L'arrivo di un ransomware è il punto di inizio: un riscatto per riavere i dati fa capire quanto sia importante la sicurezza.

Aver perso un telefonino senza password e senza un qualche meccanismo di blocco o cancellazione di autenticazioni (in banca, sul sito, all'email, etc etc, mostra come è utile avere una analisi fatta una volta che aiuti ad affrontare questi casi rapidamente dopo.

Si tratta di risparmiare, in fin dei conti.

I RISCHI NEL NON FARE NIENTE

I rischi sono nella mancata:

- gestione delle nomine e mansioni dei collaboratori
- clausole contrattuali con i fornitori sul trattamento dei dati delegato esternamente
- mancanza di informative
- mancanza di consensi documentabili
- mancata previsione del data breach
- mancata strutturazione della portabilità dei dati e della durata del trattamento

QUINDI ?

È una consulenza che costa necessariamente, ma non è detto che si debba prendere tutto subito.

Si può anche iniziare ad adempiere e farsi assistere nel tempo.

L'importante e' avere buone basi e quelle, ahime', si costruiscono studiando tanto e a lungo perche' attualmente troppi consulenti esagerano nei pericoli e negli adempimenti, e vanno tutti scremati.

In piu' i testi sono spesso in inglese (le guidelines del WP29), i consigli anche della ICO in inglese e del CNIL in francese (e dell'autorità spagnola, ottima).

Quindi cercate di capire se vi serve:

un aiuto per iniziare un aiuto per fare tutto un aiuto anche nel tempo Questo vi permettera' di investire il giusto nel giusto tempo.

Una nota: non esiste alcuna certificazione valida ai fini di legge. Solo competenza.

dott. Valentino Spataro

Consulente privacy e sviluppatore

@2018 IusOnDemand srl

[PrivacyKIT.it](https://www.privacykit.it)

e-mail:

tel: