*Caro Digitalizzatore,*

*Benvenuto nel Centro di Competenze Digitali da Pietro Montella.*

*In questa serie, scoprirai come gestire in modo esaustivo e professionale il GDPR nella tua azienda, non per sentirti obbligato a diventare un esperto (a meno che la tua aspirazione non sia proprio questa), ma per sapere esattamente cosa devi pretendere dai tuoi consulenti.*

*Non voglio fare il guru della situazione ma, in qualità di DPO e responsabile privacy per conto di tantissime aziende, devo purtroppo constatare che là fuori il caos è davvero totale.*

*Questo perché pochissime persone hanno fatto una precisa scelta di campo, mentre i più hanno finito per estendere il loro intervento in troppi ruoli, troppe specializzazioni.*

*Ma il mondo di oggi non premia i tuttologhi, come ho capito per via di esperienze vissute sulla mia pelle.*

*Per questo – a differenza di tanti altri ¬– ho scelto di specializzarmi sulle normative e sulla giurisprudenza italiana in ambito Digitale. Solo nel 2018, ho investito ingenti risorse economiche per accedere a dati, sentenze e casi studio, non solo italiani.*

*Perché se vuoi essere uno specialista, devi per forza concentrare i tuoi sforzi su competenze mirate.*

*Il mondo di oggi è troppo veloce, frenetico e selettivo per pensare di saper fare tutto. Ed è impensabile che la gente possa abboccare a facili esche di esperti superficiali e improvvisati!*

*Quindi voglio approfittare di questa "serie documentale" per condividere con te cosa ho imparato, aiutandoti a evitare gli errori più comuni che ho tipicamente riscontrato nelle aziende seguite negli ultimi 18 mesi.*

*Pietro Montella*

Ecco cosa vedremo:

1) Perché il GDPR? Da sempre sono convinto dell'importanza dei perché. Se interiorizzo il perché delle cose, so apprenderle e applicarle molto meglio, rispetto a quando mi viene detto di farlo senza un motivo comprensibile. Eccoti quindi una panoramica di tutti quei "perché" sul GDPR che tipicamente nessuno ti spiega.

2) Come applicare il GDPR attraverso il ciclo di Deming. Una metodologia che ti permette di applicare il regolamento europeo seguendo una sequenza logica per analizzare i tuoi punti di rischio, definire le tue policy e porre in essere tutti quei dispositivi che normalmente i superconsulenti vogliono farti pagare a carissimo prezzo con infinite Gap Analysis.

3) Il registro dei trattamenti: uno degli elementi *core* del GDPR. Quante ne ho viste su questo tema negli ultimi mesi! Software web miracolosi, strabilianti fogli Excel, servizi proposti a migliaia di euro. Finalmente avrai a tua completa disposizione un set di contenuti ed esempi pratici su come realizzare il TUO registro dei trattamenti, senza ricorrere a fantomatiche consulenze, canoni assurdi e tool software ai limiti dell'inutile.

4) Come fare una Risk Analysis Self Service, senza regalare soldi a sedicenti esperti di GDPR e software house che vogliono soltanto rifilarti un tool che potresti realizzare autonomamente in Excel. Ecco tutti i dispositivi base che io stesso utilizzo per le mie Gap Analysis a pagamento. Certo, troverai dei concetti semplificati e non esattamente la fotocopia di quello che faccio. Non sarebbe deontologico, non sarebbe professionale e nemmeno serio, nei tuoi confronti, farti credere che basti una lettura di qualche paginetta per sapere tutto. Ma – quantomeno – saprai tutto ciò che devi necessariamente sapere, aspettarti e pretendere da una Gap Analysis prima di cominciare

Sei pronto per questo viaggio insieme?

Allora partiamo!

# ALLA SCOPERTA DEL GDPR

Benvenuto nel primo dei quattro report che ti condurranno alla scoperta del Regolamento Europeo sulla protezione dei dati personali n. 679/2016, ma soprattutto ti aiuteranno a comprendere e applicare concretamente alla tua realtà aziendale una normativa ricca di principi di carattere generale.

In questo primo report analizzeremo le ragioni che hanno condotto all'adozione del GDPR e le principali novità.

**Perché nasce il GDPR e perché è stato adottato un regolamento in luogo di una direttiva per disciplinare il diritto alla protezione dei dati personali a differenza del passato?**

Innanzitutto il GDPR nasce con lo scopo di facilitare e rendere più sicura la circolazione dei dati, enfatizzando e ponendo quale fulcro di tutta la disciplina la tutela dei diritti degli interessati comunque coinvolti nelle attività di trattamento dei dati personali.

Il regolamento ha portata generale ed è applicabile direttamente negli stati membri senza necessità di alcun atto di recepimento, mentre la direttiva necessita di un successivo intervento legislativo affinché sia resa esecutiva all'interno dello stato membro.

L'Art. 8 della Carta dei diritti fondamentali dell'Unione Europea afferma che:

***"Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano"***

In sostanza, la costituzionalizzazione del diritto fondamentale alla protezione dei dati personali sancito dall'art. 16 del TFUE (Trattato sul funzionamento dell'Unione Europea), diritto peraltro già riconosciuto dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea, insieme alla trasposizione disomogenea della Direttiva 95/46 all'interno delle legislazioni nazionali, hanno spinto verso l'adozione di una normativa che uniformasse il diritto alla protezione dei dati personali, anche per porre un limite allo sviluppo tecnologico sempre più veloce al di fuori dell'U.E., che vede i paesi asiatici come i maggiori

produttori di hardware e gli Stati Uniti come i maggiori produttori di software. E, attualmente, è proprio attraverso l'utilizzo di smartphone, tablet e di qualunque apparecchio che possa essere collegato in rete che viene scambiata la maggior parte di informazioni.

**Cosa è cambiato rispetto al passato?**

Cambia l'approccio, o meglio la fattispecie oggetto di tutela, in quanto mentre il diritto alla riservatezza, c.d. *privacy*, rappresenta una sorta di diritto individuale, il diritto alla protezione dei dati personali estende la tutela dell'individuo oltre la sfera della vita privata e in particolare nelle relazioni sociali, così garantendo l'autodeterminazione decisionale e il controllo sulla circolazione dei propri dati.

# ACCOUNTABILITY

Non è un caso che il Regolamento Europeo sia imperniato sul principio di accountability, che di fatto sposta l'attenzione sui titolari e i responsabili del trattamento dei dati, richiedendo auto-responsabilizzazione e maggiore consapevolezza in merito alla gestione delle informazioni trattate.

Una mano a comprendere di cosa parliamo arriva dalla traduzione spagnola, dove si parla di "responsabilidad proactiva". Si aggiunge, quindi, al concetto di responsabilità anche quello di proattività. In altre parole non si può restare fermi, aspettare e lasciare che le cose accadano ma bisogna attivarsi affinché vi sia consapevolezza di come vengono gestiti i dati e le informazioni all'interno di una società e/o di una pubblica amministrazione.

È corretto sapere che il Regolamento Europeo entra in vigore nel maggio del 2016 per diventare esecutivo in tutti gli stati membri il 25 maggio 2018, data che viene ricordata come un incubo per tutti i possessori di una casella di posta elettronica.

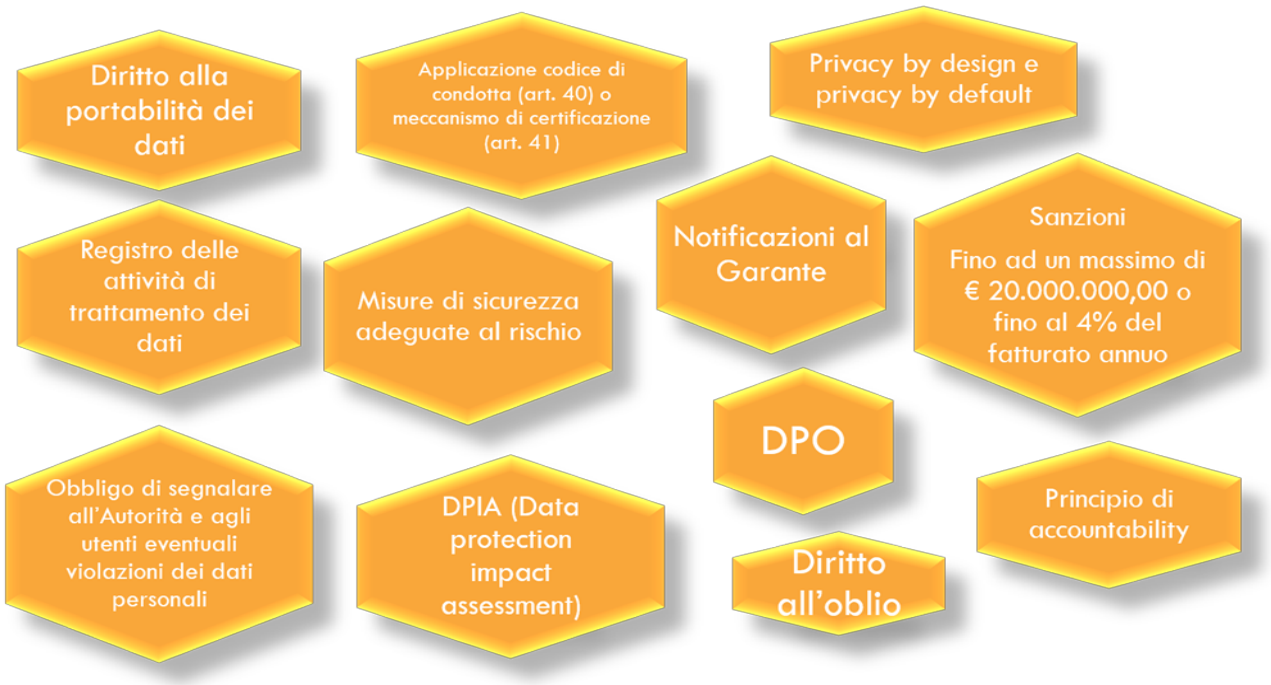
Ed ecco un primo errore che è stato commesso da moltissime aziende che, senza curarsi della "bontà" dei propri database, hanno inviato mail richiedendo il consenso al trattamento dei dati sulla base della nuova informativa redatta ai sensi degli articoli 13 e 14 del Regolamento Europeo n. 679/2016.

**Perché dico che è stato commesso un errore?**

**La risposta è banale.**

Se una qualunque azienda non aveva il consenso al trattamento dei dati di una persona prima del 25 maggio 2018, significa che probabilmente l'utilizzo di quei dati non era lecito, per cui lo stesso invio di e-mail, magari attraverso software di marketing automation, era illecito anche se effettuato per chiedere il consenso a continuare a trattare dei dati ottenuti chissà come e dove.

Nel grafico che segue si evidenziano le più importanti novità previste dal General Data Protection Regulation n. 679/2016:




Soffermiamoci un attimo sulle notificazioni al Garante privacy. Cosa cambia?

Ecco una prima applicazione concreta dell'accountability.

Cambia il modo di comunicare con l'Autorità in quanto oggi, a dispetto di quanto accadeva in passato, quando si decide di iniziare un trattamento che potrebbe comportare dei rischi per la protezione dei dati delle persone fisiche non è più necessario rivolgersi preventivamente al Garante.

I controlli e le valutazioni sulla compliance al GDPR saranno effettuati ex post in sede di ispezione.

E ancora:

- l'obbligo di "privacy impact assessment" (valutazioni preventive di impatto sulla tutela dei dati) in caso di trattamenti rischiosi, quindi una analisi dei rischi puntuale. Tra l'altro, il testo del regolamento cita espressamente i parametri gravità e probabilità dell'evento, cioè è necessario effettuare una corretta e puntuale analisi dei rischi;

- cambiano le responsabilità sia dei Titolari che dei Responsabili;

- l'obbligatorietà di nominare il DPO, "data protection officer" (responsabile della protezione dei dati personali), al quale sarà richiesto ai sensi dell'art. art 37 paragrafo 5 il possesso di elevate competenze e qualità professionali e "*in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.*";

- il diritto all'oblio, per cui ogni interessato potrà richiedere la rimozione di propri dati personali per motivi legittimi, cioè perché l'informazione non è più attinente;

- l'istituzione dei registri dei trattamenti, ovvero dei documenti di sintesi sui trattamenti effettuati, le misure di sicurezza adottate, i rischi relativi;

- la previsione delle figure dei "joint controllers" (titolari congiunti), che potranno "spartirsi" le responsabilità privacy in un apposito contratto, di cui si dovrà tenere conto in caso di controlli o contenziosi: questa novità sarà d'aiuto, in particolare, nel settore del cloud computing providing (fino a oggi difficilmente inquadrabile nei vecchi schemi titolare/responsabile);

- la previsione del concetto di "stabilimento principale" del titolare, per evitare che un'impresa attiva in più Stati UE debba fronteggiare gli adempimenti nazionali di ogni singolo Stato;

- la previsione del ruolo di "lead authority", in modo tale che vi sia un solo Garante di volta in volta responsabile dei procedimenti multi-Stato;

- sanzioni molto più pesanti, fino al 4% del volume d'affari globale di un'impresa (o 20.000.000,00 €), per assicurare che la protezione dei dati inizi a diventare un tema sensibile anche per i consigli di amministrazione di grandi colossi multinazionali;

- l'introduzione del principio della cosiddetta "accountability", per il quale ogni titolare, in caso di problemi o controlli, dovrà dimostrare nei fatti, al di là dei formalismi, di avere adottato i modelli organizzativi e le misure di sicurezza logiche, fisiche, elettroniche per proteggere i dati;

- l'obbligo di attenersi, nell'ideazione di nuovi prodotti o servizi, ai principi della "data protection by design" e della "data protection by default", cioè l'applicazione di principi di project management alla privacy;

- notificazione dei data breach, ovvero la segnalazione, entro 72 ore, di un trattamento non corretto e/o errato, all'autorità ed all'interessato.

Si può quindi notare una forte attenzione sul ruolo centrale della tutela dei dati personali, come recita il considerando 3 bis del regolamento:

3 bis) *Il Trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea e sanciti dai trattati, in particolare il diritto al rispetto della vita privata e familiare, del domicilio e delle comunicazioni, il diritto alla protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, così come la diversità culturale, religiosa e linguistica.*

Nel prossimo white paper ci occuperemo del metodo da applicare per rendere processi aziendali compliance al GDPR 679/2016.

*Nel prossimo episodio….*

*Quali sono gli strumenti che un consulente legale, specializzato in normative e giurisprudenza del mondo digitale, utilizza per mappare i livelli di rischio della tua impresa.*

*Nel prossimo episodio, vedrai svelati alcuni segreti che ti renderanno più autonomo nella definizione dei tuoi rischi da GDPR, e più consapevole al cospetto delle consulenze che hai ricevuto o riceverai. Vai al secondo capitolo di questa serie e che il Digitale sia con Te!*

## *COSA VUOI FARE ADESSO?*

| *CHIEDO UN APPROFONDIMENTO ALLO STAFF LEGALE DEL CENTRO DI COMPETENZE DIGITALI* | *VADO AL PROSSIMO CAPITOLO DI QUESTO WHITEPAPER* |
|---|---|
| CLICCA QUI | CLICCA QUI |