Cosa è necessario sapere

GDPR: il Regolamento UE 2016/679 in Sintesi

Il nuovo regolamento europeo (UE) 2016/679 per la Protezone dei Dati GDPR *(**G**eneral **D**ata**P**rotection **R**egulation)* determina le *"linee guida"* da adottare in materia di *Protezione delle Persone Fisiche* con riguardo al **Trattamento** dei **Dati** nonché alla *libera circolazione* di tali dati.

È importante sottolineare il fatto che, bensì l'obbligo sia per **tutte** le **aziende**, i **"Dati"** a cui si riferisce il Regolamento sono quelli che riconducono o che si possono in qualche modo ricondurre a **Persone Fisiche** e non giuridiche (aziende).

Con il regolamento Europeo in materia di protezione dei dati personali (regolamento 2016/679), approvato in data 14 aprile 2016 dal Parlamento Europeo e pubblicato sulla Gazzetta Ufficiale Europea del 4 maggio 2016 inizia una nuova stagione per i diritti dei cittadini europei nei rapporti con le pubbliche amministrazioni e le imprese.

Il regolamento costituisce un prezioso tentativo di armonizzazione delle regole privacy dei vari Stati ed è finalizzato a sviluppare il mercato unico digitale attraverso la creazione e la promozione di nuovi servizi, applicazioni, piattaforme e software.

Il regolamento costituisce con la direttiva Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati il c.d. "**pacchetto protezione dati personali".**

Il testo del regolamento abroga la direttiva la Direttiva 95/46/Ce in materia di protezione dei dati personali /privacy, concepita in un periodo nel quale solo una minima parte della popolazione europea (nella percentuale del 1%) utilizzava internet e non esistevano social media, tablet, app e gli scenari e gli effetti della moderna e l' attuale società della sorveglianza elettronica nella quale sono gli stessi cittadini che pubblicano, più o meno inconsapevolmente i propri dati personali sulle piattaforme on line e social media.

RGPD (Regolamento Generale Protezione Dati) UE 2016/679

E che fine farà l'attuale "Legge Privacy" Dlgs 196/2003?

L'attuale Legge Italiana *D.lgs 196 del 2003, meglio conosciuta come "Legge Privacy",* è stata abrogata definitivamente nel Marzo scorso.

Sono comunque attualmente in corso di emanazione, da parte del **Garante Privacy**Italiano, nuove norme integrative che dovrebbero *"raccordarsi"* e fare "*maggiore chiarezza"* sul nuovo Regolamento Europeo.

Il Regolamento UE 2016/679 GDPR abroga completamente la vecchia Direttiva 95/46, dalla quale sono nate tutte le Leggi Privacy dei vari Stati Membri, tra cui anche la nostra Dlgs 196/2003.

Trattandosi appunto di "*Regolamento"* e non di "*Direttiva"*, il GDPR non è soggetto stavolta a *"recepimento"* e *non potrà quindi essere modificato* dagli Stati Membri, né sul contenuto né, tanto meno, sulle date di applicazione essendo **applicabile, fin dall'inizio, esattamente così com'è**.

Le aziende che avevano già adottato a suo tempo le misure previste nella "Legge Privacy" come, ad esempio, il *DPS* o *Documento Programmatico della Sicurezza (poi tolto dal 2013)*, saranno sicuramente avvantaggiate perché non dovranno partire da zero, se non altro come "cultura" da introdurre in azienda.

I **VANTAGGI** del Nuovo Regolamento UE 2016/679 o GDPR sono:

Con questo Regolamento, il Consiglio Europeo, oltre ad *armonizzare* e ad *aggiornare*le normative privacy in tutta la UE, si pone come secondo obiettivo, quello di ridefinire l'*approccio delle aziende in materia di protezione dati,* in virtù dei continui attacchi informatici di cui sono oggetto da alcuni anni le imprese di ogni dimensione e settore, fornendo una *guida utile* anche in questa direzione.

I principali **vantaggi** del GDPR sono:

- *norme uniche per tutta l'UE*
- *condizione di parità per tutte le imprese UE*
- *norme adatte alla web-economy*
- *norme "scalabili" ed "adattabili" ai cambiamenti tecnologici ed ai futuri scenari economici.*

Le principali **DIFFERENZE** del GDPR rispetto all'attuale *"Legge Privacy" D.lgs 196/2003*

La novità principale del nuovo regolamento è che sparisce il concetto di *"MISURE MINIME"* , alla base dell'attuale normativa D.Lgs 196, per lasciare il posto a quello di **"MISURE ADEGUATE".**

Ma, la vera *rivoluzione*, è l'introduzione del nuovo principio di **"ACCOUNTABILITY"***(Responsabilizzazione)*.

Tale principio di fatto attribuisce più **discrezionalità** ma, al tempo stesso, **maggiore responsabilità** al *"Titolare del Trattamento"* su tutto quello che concerne la *protezione dati* con un inasprimento consistente delle *sanzioni previste* in caso di inadempienza.

Se è vero che viene lasciato più spazio alla *discrezionalità* è anche vero che, il *Titolare*ed il *Responsabile del Trattamento* hanno il preciso **dovere** di **dimostrare** le **ragioni**che hanno determinato le scelte fatte.

Gli impatti del regolamento ue 2016/679 su cittadini e PA

Quali sono le principali novità per i cittadini? E quali sono gli impatti per la pubblica amministrazione?

I cittadini, con le nuove disposizioni, sono al centro del sistema; sono riconosciuti ai cittadini: il **diritto alla portabilità dei dati, il diritto all'oblio (riconosciuto fino ad ora solo a livello giurisprudenziale), il diritto di essere informato in modo trasparente, leale e dinamico sui trattamenti effettuati sui suoi dati e di controllare, il diritto di essere informato sulle violazioni dei propri dati personali ("data breach", notificazione di una violazione di dati). Il testo in esame riconosce, pertanto, un livello elevato e uniforme di tutela dei dati ed è finalizzato a dare un maggiore controllo ai cittadini sull'utilizzo dei loro dati.**

Il regolamento comporta un cambiamento anche culturale: difendere i dati, significa difendere le persone, l' identità e la libertà delle stesse.

I cittadini hanno il diritto di essere avvertiti dalle pubbliche amministrazioni e dalle imprese delle violazioni dei loro dati personali (data breach notification) entro le 72 ore, obbligo previsto attualmente solo in alcuni settori (fascicolo e dossier sanitario, interscambio di dati fra le pubbliche amministrazioni, Tlc e settore bancario)

I cittadini hanno il diritto di dare mandato a un organismo, un'organizzazione o **un'associazione senza scopo di lucro,** che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per loro conto e di esercitare per loro conto i diritti sui propri dati (v. artt. 77, 78 e 79) nonché, il diritto di ottenere il risarcimento dei danni causato dalla violazione del regolamento.

Il testo impone alle imprese e alle pubbliche amministrazioni una forte responsabilizzazione, un cambio di passo, un approccio proattivo, la protezione dei dati personali diventa, finalmente, un asset strategico delle pubbliche amministrazioni che deve essere valutato prima, già nel momento di progettazione di nuove procedure, prodotti o servizi, (**principi data protection by design" e "data protection by default**) senza derive burocratiche che hanno negli anni passato relegato la protezione dei dati personali ad un mero adempimento formale di mettere una firma per presa visione dell'informativa o per il consenso al trattamento di dati sanitari: con il regolamento si torna alla concretezza.

Le pubbliche amministrazioni hanno, a seguito delle disposizioni del regolamento europeo, l'obbligo prima di procedere al trattamento, di effettuare una **valutazione dell'impatto** ("privacy impact assessment"), dei trattamenti previsti dal regolamento quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La valutazione di impatto privacy richiede una puntuale e documentata analisi dei rischi per i diritti e le libertà degli interessati.

Il regolamento europeo introduce alcune **semplificazioni** degli oneri e adempimenti a carico delle pa.: viene abrogato l'adempimento della notificazione preliminare al Garante privacy, dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante per la protezione dei dati personali l'esistenza di un'attività di trattamenti dati particolarmente delicati (es. dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica; dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria etc..).

Con il nuovo testo del regolamento in materia di protezione dei dati personali entra nel nostro ordinamento il "**principio di accountability**" (obbligo di rendicontazione): le pubbliche amministrazioni titolari del trattamento dei dati devono dimostrare:

– di avere adottato le misure di sicurezza adeguate ed efficaci a protezione dei dati e, costantemente riviste e aggiornate e che le proprie attività;

– trattamenti sono conformi con i principi e le disposizioni del regolamento europeo, compresa l'efficacia delle misure.

Il regolamento prevede che**l'adesione ai codici di condotta** (v.art.40) o a un meccanismo di certificazione (v. art.42) può essere utilizzata come elemento per dimostrare il rispetto degli

obblighi del titolare del trattamento (altri elementi di forte innovazione rispetto alla normativa precedente).

Al fine di poter dimostrare la conformità alle disposizioni del regolamento, viene previsto l'obbligo del titolare o del responsabile di **tenuta di registro delle attività di trattamento** effettuate sotto la propria responsabilità con relativa descrizione delle misure di sicurezza (art. 30).

Il regolamento specifica che il registro (in formato anche elettronico) deve contenere una descrizione generale delle misure di sicurezza tecniche e organizzative e che su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento sono tenuti a mettere il registro a disposizione dell'autorità di controllo.

Si osservi che il sopra citato adempimento obbligatorio per le pubbliche amministrazioni è molto più rigoroso e puntuale del precedente obbligo di adozione del Documento programmatico per la sicurezza (DPS), adempimento abrogato dal Decreto Monti.(decreto-legge 9 febbraio 2012, n. 5).

In riferimento al profilo della sicurezza del trattamento, il regolamento prevede (v.art. 32) che il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei **costi di attuazione**, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Il profilo del costo di attuazione delle misure di sicurezza costituisce una novità importante per il nostro ordinamento.

Il DPO del regolamento UE 2016/679

Il regolamento introduce nel nostro ordinamento una nuova figura il "**data protection officer"** (responsabile della protezione dei dati personali) che le pubbliche amministrazioni hanno l'obbligo di nominare al proprio interno e deve sempre essere "coinvolto in tutte le questioni riguardanti la protezione dei dati personali".

Il **data protection officer (DPO)** deve essere in possesso di specifici requisiti: competenza, esperienza, indipendenza e autonomia di risorse, assenza di conflitti di interesse e dovrà presidiare i profili privacy organizzativi attraverso un'opera di sorveglianza sulla corretta applicazione del regolamento europeo, della normativa privacy e sulla normativa interna, sull'attribuzione delle responsabilità, informazione, sensibilizzazione e formazione del personale, informazione, consulenza e rilascio di pareri.

Il data protection officer che potrà essere sia interno che esterno all'ente sarà tenuto a presidiare i profili privacy, cooperare con l'Autorità Garante e riferisce direttamente al vertice gerarchico del titolare del trattamento.

Il Data protection officer costituisce u**n punto di riferimento e di contatto per i cittadini** che possono rivolgersi per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal regolamento europeo. L'identità ed i dati di contatto del data protection officer devono essere riportati, nell'ottica di trasparenza verso i cittadini, nell'informativa privacy (art. 13, primo comma, lett.b) da rendere prima del conferimento dei dati da parte dei cittadini, devono essere pubblicati sul sito dell'ente (art.37) e contenuti anche nel registro dei trattamenti.

Nell'eseguire i propri compiti il data protection officer considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il testo prevede inoltre un rafforzamento dei poteri delle Autorità Garanti nazionali e un **inasprimento** delle sanzioni amministrativo a carico di imprese e pubbliche amministrazioni: nel caso di violazioni dei principi e disposizioni del regolamento, le sanzioni, in casi particolari possono arrivare fino a 10 milioni di euro o per le imprese fino al 2%-4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Nei due anni di transizione verso l'applicazione del nuovo regolamento privacy, il Garante per la protezione dei dati personali svolgerà un ruolo chiave, nella complessa opera di armonizzazione delle normativa nazionale in materia di protezione dei dati personali oggi vigenti e dei propri precedenti provvedimenti generali dal forte impatto sulle pubbliche amministrazioni (posta elettronica ed internet, videosorveglianza, amministratori di sistema, trasparenza on line) rispetto ai nuovi principi, istituti e responsabilità previsti dal nuovo testo.

Il regolamento costituisce un punto di partenza verso il traguardo comune di un livello uniforme ed elevato di protezione dei dati personali dei cittadini al fine di rafforzare la fiducia, la certezza legale e la concorrenza nell'ottica di costruire un nuovo dialogo con i cittadini, sviluppare servizi on line, attraverso l'aumento della fiducia delle persone nelle transazioni o line.

La protezione dei dati personali, costituisce, alla luce del nuovo regolamento, una pietra angolare nella progettazione dei servizi, programmi, software e dei processi aziendali anche delle pubbliche amministrazioni.

Il regolamento richiede alle pubbliche amministrazioni di andare oltre le regole e gli aspetti formali: i dirigenti, funzionari devono essere attori di un profondo cambiamento culturale con forte impatto organizzativo nell'ottica di adeguare le norme di protezione dei dati ai cambiamenti determinati dall'incessante evoluzione delle tecnologie (cloud computing, digitalizzazione, social media, cooperazione applicativa, interconnessione di banche dati, pubblicazione automatizzata di dati on line) nelle organizzazioni pubbliche.

Quali sono le AREE su cui INTERVENIRE per il GDPR

Quali sono i **CONCETTI CHIAVE** del GDPR da tenere a mente

Cominciamo a prendere confidenza con le *denominazioni* e i *concetti* che più incontreremo quando ci ritroveremo a parlare di GDPR.

I **SOGGETTI** del trattamento nel nuovo GDPR:

- **INTERESSATO al Trattamento**: la *persona fisica* oggetto del trattamento dati
- **TITOLARE del Trattamento**: la *persona fisica* o *giuridica* (azienda/ente) titolare del trattamento
- **RESPONSABILE del Trattamento**: la *persona fisica* o *giuridica* responsabile di un determinato trattamento. Può essere anche esterno mediante nomina (*es. dati in Hosting, provider di posta, servizio paghe..)* o interno *(es. resp. reparto/processo interno o lo stesso Titolare del Trattamento)*
- **DPO** *(Data Protection Officer)* o *RPD* (Responsabile Protezione Dati) o *Privacy Officer*: è la *nuova figura* introdotta nel 2016 dal GDPR. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

- Entrambi, *Titolare* e *Responsabile*, rispondono legalmente.
- Possono essere nominati anche *più responsabili del trattamento.*

Il Principio di "ACCOUNTABILITY" nel GDPR

il GDPR pone l'accento sui concetti di **"Responsabilizzazione"** *(Accountability)* e di **"Misure Adeguate"** in quanto, il *Titolare del Trattamento* deve **garantire** ed essere sempre in grado di **dimostrare** di *rispettare* i *princìpi del Regolamento* nonché, di aver messo in atto le *misure ritenute idonee dal Titolare stesso*

Anche se nel GDPR sparisce il concetto di "Misure Minime", presente nel D.lgs 196/2003, si può comunque prevedere un insieme minimo di azioni per soddisfare le esigenze di *Accountability* il cui nucleo potrebbe essere così composto:

- ***Assessment:*** *valutazione iniziale legale e informatica*
- ***Registro dei Trattamenti:*** *non obbligatorio fino a 250 dipendenti ma, "caldamente consigliato"*
- ***Funzionigramma privacy:*** *definizione Ruoli e Compiti*
- ***Risk Assessment:*** *valutazione del rischio sul dati da trattare*
- ***Privacy Impact Assessment****: distinte valutazioni sull'impatto privacy relative a particolari processi, servizi, prodotti, sistemi che il Titolare può adottare, installare o fornire (ad es: installazione di impianti di videosorveglianza o di gps; organizzazione di campagne marketing; ecc.)*
- ***Documentazione****: Informative, consensi e nomine*
  Formazione*: adeguata istruzione a chi dovrà trattare i dati*
- **Gestione:** *mediante audit periodici di controllo*

Il GDPR introduce un NUOVO RUOLO: il DPO

Il GDPR prevede l'inserimento di un nuovo ruolo nell'organigramma:
il **Responsabile**della **Protezione Dati** o ***DPO*** *(Data Protection Officer)* detto anche **Responsabile** della**Sicurezza** *(Privacy Officer).*

CHI è il DPO

Il **DPO** è una nuova *figura specialistica*, con cognizioni *tecniche*, *informatiche* e *giuridiche.*

Viene *nominato* dal *Titolare del Trattamento* e, il suo compito, è quello di **supportare** il **Titolare** nell'applicazione delle procedure che riguardano il nuovo regolamento fungendo anche da *interfaccia* fra le *Autorità di Controllo* e i diretti interessati.

I **COMPITI** del *DPO*

- ***Informare*** *e fornire* ***consulenza*** *al titolare del trattamento nonché ai dipendenti;*
- ***Sorvegliare*** *l'osservanza del Regolamento GDPR*
- *Fornire, se richiesto, un parere in merito alla* ***valutazione d'impatto*** *sulla protezione dei dati;*
- ***Cooperare*** *con l'****Autorità di controllo*** *(il Garante Privacy);*
- *Fungere da* ***punto di contatto*** *per l'****Autorità di controllo*** *per questioni connesse al trattamento;*

QUANDO devo nominare un DPO

La designazione del DPO è *obbligatoria* per tutti gli *enti pubblici* mentre, per le *aziende private* solo per le seguenti *tipologie* di trattamenti:

- *effettuati su larga scala e sistematici (Es. Marketing, Profilazione..etc)*
- *comandati da una Pubblica Autorità*
- *che riguardano particolari categorie di dati sensibili*

Anche se la nomina del DPO è, nella maggior parte dei casi facoltativa, se ne consiglia comunque l'introduzione, per **agevolare** l'**inserimento,** il **monitoraggio** e la **corretta applicazione** delle procedure nonché, per **gestire** ed **aggiornare** tutta la **documentazione** necessaria.

Inoltre il DPO assume un ruolo fondamentale, in caso di *violazione dei dati (Data Breach),* come interfaccia con le *Autorità di Controllo*.

INQUADRAMENTO del DPO

Il Responsabile della Protezione dei Dati può essere:

- *un **dipendente** del titolare del trattamento o del responsabile del trattamento*
- *oppure assolvere i suoi compiti in base a un **contratto di servizi***

DPO e altri **Ruoli Manageriali:** *possibile "Conflitto d'interesse"?*

La materia, che sicuramente richiede anche *competenze tecnico/sistemistiche*, sta generando il dubbio in molte aziende sul fatto di delegare o meno il ruolo del **DPO** ad **altri Ruoli Manageriali** interni come ad es. il *Responsabile IT* o il *Direttore Marketing***,** o a *partner informatici* esterni qualora non esistano questi ruoli all'interno.

È chiaro che il *Responsabile CIO/Marketing* o il *Partner IT* avrebbero un compito determinante nel supportare la privacy, vista la profonda conoscenza dell'infrastruttura dell'azienda, motivo per cui sono da considerare **figure chiave** all'interno di un *progetto Privacy*.

È opinione condivisa però che, nel caso del doppio ruolo, il *Resp.IT/DPO* si troverebbe a svolgere contemporaneamente il ruolo di *controllore* e *controllato*, generando quindi un possibile *conflitto d'interesse*.

A tal proposito il "*Gruppo di Lavoro Art.29" del Garante Privacy* precisa nelle linee guida sul DPO che:

*"...A grandi linee, possono sussistere situazioni di **conflitto all'interno dell'organizzazione** con riguardo a ruoli manageriali di vertice (**amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT**), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento…"*

AREE e RUOLI di un PIANO PRIVACY GDPR

Un **Progetto Privacy,** per essere *serio* e *sostenibile*, deve essere *condiviso* in *primis* dai **vertici aziendali** per essere esteso, progressivamente, a tutti gli *stakeholder* e *reparti* che, in qualche modo, hanno a che fare con quei processi che trattano dati personali *(Es. paghe, marketing, commerciale, amministrazione, Risorse Umane HR etc.).*

Un adeguato progetto GDPR deve coinvolgere più ruoli, competenze e reparti interni ed esterni all'azienda

COME PROCEDERE per un piano Privacy GDPR:

la FASE iniziale

1. Porre le BASI

Abbiamo detto prima che è necessario coinvolgere molte aree dell'azienda prima fra tutte la Dirigenza.

In questa PRIMA FASE è importante coinvolgere, oltre ai **Dirigenti**, anche i **Key User s**ono responsabili dei vari processi e reparti che più di tutti interverranno nel progetto.

In questo step è necessario individuare bene gli obiettivi e porsi le seguenti **domande chiave**:

*Quali sono gli **OBIETTIVI** di business a medio e lungo termine dell'azienda?*

*Quali **DATI** servono per raggiungere questi obiettivi?*

2. Mappare i dati e fare l'analisi delle lacune

In questa è importante **rilevare** e **documentare** quali dati personali sono in possesso dell'azienda, *da dove provengono*, *da chi*, *dove* e *come* vengono gestiti questi dati, rendendone *consapevoli* i vari *team* coinvolti.

Quesiti fondamentali per mappare i dati:

1. *Che **TIPI** di **dati** raccogli?*
2. ***PERCHÈ** li raccogli?*
3. ***DOVE** archivi i tuoi dati?*
4. ***CHI** ha accesso a questi dati?*
5. *Per **QUANTO TEMPO** vengono conservati?*
6. *Vengono rispettati i **Diritti Privacy** delle persone?*

Una volta mappati i DATI bisogna individuare le **lacune** quindi **COSA MANCA** *(GAP ANALYSYS)* per colmare queste lacune e rendere **adeguate** le procedure alle disposizioni del GDPR e, sottolineiamo "*adeguate"*, ricordando che il GDPR non prevede il concetto di *"misure minime"* presente invece nell'attuale normativa "privacy".

3. **VALUTARE** i **RISCHI** – *Risk Assessment*

Una volta che abbiamo capito cosa manca è necessario definire quali saranno le **AZIONI NECESSARIE** per *adeguare* le attuali procedure di trattamento e renderle conformi entro la data di applicazione del **25 Maggio 2018** nonchè, quello che serve per *aggiornarle* e *manutenerle* anche dopo tale termine.

Nel #GDPR ciascuna azienda deve effettuare una propria analisi dei rischi ed eseguire azioni specifiche atte a ridurre al minimo il rischio basandosi su moderni principi come "Privacy By Design" e "Privacy By Default"

4. Creare una ROADMAP

Bene, arrivati a questo punto, abbiamo stabilito quali sono gli obiettivi e le priorità, abbiamo definito lo scenario e deciso come agire in base ad un'Analisi specifica dei Rischi in base ai *dati* ed al *rischio per il loro trattamento.*

Ora è necessario realizzare che ognuna di queste azioni confluirà in un *progetto specifico*, ognuno con un suo *responsabile*, *risorse assegnate*, *competenze* e *scadenze*.

Una vera e propria **ROADMAP** con le *azioni* da *eseguire*, da *chi* (definizione ruoli e competenze), in *che modo* e in che *tempi*, la *documentazione* da produrre, le *comunicazioni* interne ed esterne, gli *interventi infrastrutturali (IT)*, ed infine la *formazione* e la *consulenza* ai responsabili ed al personale.

5. AGIRE

Adesso che abbiamo *coinvolto*, *analizzato*, *rilevato*, *descritto* e *definito "cosa fare"* è arrivato finalmente il momento di **mettere in pratica** tutto quello che si è detto.

Innanzitutto è fondamentale che tutti i *Ruoli* siano ben chiari e definiti ed ogni cosa vada nella direzione giusta.

In questa fase il ruolo di *supervisione* e *coordinamento* del **DPO** è fondamentale, non solo per *controllare* e *sorvegliare* ma, anche per fornire *consulenza* e *formazione* alle risorse coinvolte e, sopratutto per **monitorare,** con l'ausilio di strumenti di *"Audit",*che non ci siano **violazioni** dei **dati** nel qual caso, dovrà prontamente intervenire per **gestire** il **Data Breach** con le Autorità di Controllo.

Che cos'è l'OBBLIGO di NOTIFICA o DATA BREACH NOTIFICATION

Una delle più importanti novità introdotte e che, al di là delle importanti *sanzioni* previste, induce più di tutte a prendere sul serio il GDPR, è proprio l'**Obbligo** di **Notifica** o *Data Breach Notification.*

In caso di **Violazione dei Dati**, dal 25 Maggio 2018 non sarà più possibile nascondersi dietro il "silenzio" ma, sarà **obbligatorio denunciare** l'accaduto alle Autorità Competenti (Garante Privacy) e ai diretti interessati, entro un limite massimo di **72 ore** dalla scoperta.

..ma non finisce qui!!

Infatti *non è sufficiente "limitarsi" a denunciare* perché, se si vuole limitare le sanzioni, è necessario essere anche in grado di **dimostrare** documentando che si è fatto tutto quello che si poteva fare per *limitare al minimo possibile il danno*.

Il #GDPR può essere lo stimolo che serviva alle aziende per mettere in sicurezza il proprio patrimonio di dati.

Perché adeguarsi al GDPR?

E poi, mi conviene investire in CYBERSECURITY?

Sono i quesiti che si stanno ponendo un po' tutti, sopratutto le *piccole* e *medie aziende*, che vedono nel GDPR l'ennesima *"trappola burocratica"*, *solo costi e niente vantaggi*.

Cercheremo di dare una risposta ragionando al contrario e cioè; quanto potrebbe costare ad un'azienda *non investire* sul GDPR?

Ma quanto mi può costare un progetto per adeguarmi al GDPR?

Prima di chiedersi quanto può costare adeguarsi al GDPR non è forse il caso prima di chiedersi *quanto potrebbe costare una perdita di dati* alla tua azienda?

Una **violazione** della **sicurezza** che comportasse una *perdita* di *dati importante* può essere **devastante**, anche in una piccola azienda, per vari motivi riassunti in questa infografica:

Le SANZIONI PREVISTE

Le **sanzioni** previste dal Regolamento Europeo 2016/679 non sono di poco conto anzi..

- Fino a **20 Milioni** di €uro
- Fino al **4% del fatturato** mondiale annuo

A queste si devono poi aggiungere le possibili implicazioni *penali* previste dalla legislazione del paese in caso di violazione grave, a cui sarebbero soggetti sia il *Titolare* (legale rappresentate) che il *Responsabile del Trattamento* se separati.