Che cos'è il GDPR

Il termine GDPR contiene le iniziali delle parole inglesi "**General Data Protection Regulation**" che significano letteralmente "**Regolamento generale per la protezione dei dati personali**".

Pertanto il termine GDPR non identifica una parola utilizzata nel settore del marketing (come "ROI" o "KPI") ma bensì un testo normativo. *Il GDPR infatti è un regolamento europeo divenuto operativo negli Stati membri dell'Unione Europea in data 25 maggio 2018.*

Il *legislatore europeo* ha deciso di utilizzare uno strumento molto incisivo e cioè un "**regolamento**" per disciplinare in modo omogeneo il trattamento dei dati personali. I regolamenti, infatti, si caratterizzano per essere direttamente applicabili negli Stati membri al pari delle leggi nazionali; questo significa che quando il Parlamento europeo approva un regolamento, tale atto diventa vincolante nel nostro Paese come se fosse una legge emanata dal Parlamento italiano.

Questa situazione ha generato un vero e proprio "allarme gdpr" dal momento che molte aziende e professionisti si sono dovuti affrettare per adeguarsi il prima possibile alla normativa europea. Il GDPR, infatti, ha avuto un impatto significativo per tutti coloro che gestiscono un sito web e trattano quotidianamente i dati dei loro utenti; sono ancora molte le imprese italiane che non risultano conformi alle regole del GDPR e che devono completare il processo di adeguamento.

A tale proposito si parla infatti di "**compliance al GDPR**" da parte dei soggetti obbligati.

Ma cosa vuole dire essere compliance al GDPR?

Il termine "compliance" significa letteralmente "**conformità**" ed in questo caso indica la corrispondenza della propria attività con le regole inderogabili indicate nel GDPR. Se vuoi sapere cosa devi fare per rendere il tuo sito internet "compliance" al GDPR continua a leggere questa guida.

Come è composto il GDPR?

Il GDPR è un **regolamento composto da 99 articoli** e si divide in 11 parti (**CAPI**) che trattano i seguenti argomenti:

- *Disposizioni generali*
- *Principi*
- *Diritti dell'interessato*
- *Titolare del trattamento e responsabile del trattamento*
- *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*
- *Autorità di controllo indipendenti*
- *Cooperazione e coerenza*
- *Mezzi di ricorso, responsabilità e sanzioni*
- *Disposizioni relative a specifiche situazioni di trattamento*
- *Atti delegati e atti di esecuzione*

- *Disposizioni finali*

I 99 articoli del GDPR sono preceduti da 173 paragrafi che prendono il nome di "**Considerando**"; una corretta applicazione delle regole del GDPR non può prescindere dall'attenta analisi dei "considerando".

Ma cosa sono i "Considerando" del GDPR?

Si tratta di indicazioni di fondamentale importanza che aiutano a **capire meglio il testo del GDPR**; pertanto, per comprendere come adeguarsi al regolamento europeo è necessaria una lettura integrata e ragionata dei Considerando e degli articoli.

Quali dati protegge il GDPR?

Il GDPR disciplina il trattamento dei "dati personali" di soggetti che si trovano all'interno dell'Unione Europea.

Per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile.

Per "identificabile" si intende la persona fisica che può essere riconosciuta, direttamente o indirettamente. Ad esempio, una foto oppure il riferimento al nome e cognome consentono di identificare una persona in modo diretto; mentre l'indicazione del codice fiscale o dell'indirizzo IP del computer sono elementi che permettono di risalire indirettamente all'identità di una persona.

Il GDPR offre una tutela speciale ai c.d. "**dati personali particolari**" (ex "dati sensibili") e cioè quei dati personali idonei a

rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale. Tuttavia nel regolamento europeo questi dati non vengono definiti sensibili come in passato ma vengono semplicemente chiamati "categorie particolari di dati personali".

Cambia il nome ma non la sostanza: **il GDPR tutela i dati particolari introducendo specifiche limitazioni al loro trattamento.**

Il regolamento europeo fa rientrare in questa categoria anche i seguenti dati:

- **Dati genetici**: ottenuti tramite analisi di DNA ed RNA da un campione biologico della persona fisica;
- **Dati biometrici**: come ad esempio le impronte digitali, grazie ai quali è possibile identificare una ed una sola persona fisica;
- **Dati sulla salute**: sono le informazioni relative allo stato di salute fisica e/o mentale di un soggetto comprese tutte le diagnosi passate, attuali o future.

Sarà importante ricordarlo se effettui attività di marketing per aziende mediche o farmaceutiche.

La persona a cui si riferiscono i dati oggetto del trattamento si definisce "**interessato**".

È importante ricordare che **l'interessato può essere solo una persona fisica e non un'azienda**.

Quali sono i soggetti obbligati?

Il GDPR si applica a 3 categorie di soggetti:

- *i privati e le società che trattano dati personali di soggetti che si trovano all'interno dell'Unione Europea*;
- *i privati e le società indipendentemente dal fatto che il trattamento stesso sia effettuato o meno nell'UE;*
- *i privati e le società stabiliti al di fuori dell'Unione Europea ma che trattano dati personali di soggetti che si trovano nell'Unione Europe*.

Ai fini dell'applicazione o meno del GDPR vengono adottati due criteri.

Il primo è il c.d. "**Establishment Criterion**" e cioè il principio di "**stabilimento**".

In questo caso ciò che conta per innescare l'applicazione del GDPR è la presenza in Europa del soggetto che tratta i dati personali per mezzo di uno stabilimento. Un'informazione da ricordare se svolgi attività di marketing per grandi multinazionali. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. Quindi se la sede o una filiale della tua

azienda si trova in Italia, Francia, Spagna o altro paese dell'Unione Europea devi rispettare le regole del GDPR.

Il secondo criterio adottato è quello Il "**Targeting Criterion**", e cioè il principio della collocazione fisica e geografica di tutti i soggetti destinatari del trattamento. Infatti Il GDPR si applica quando:

- il trattamento si riferisce all'offerta di beni o servizi a soggetti interessati dell'UE;
- il trattamento coinvolge il monitoraggio del comportamento di soggetti interessati dell'UE.

Quindi anche se ad esempio la sede della tua azienda si trova in America o in Australia ma tratti dati personali di soggetti che si trovano nell'Unione Europea (attività di profilazione, remarketing, retargeting etc) **devi rispettare le regole del GDPR**.

Andando avanti ti spiegheremo questo concetto in modo più approfondito.

Il GDPR, invece, non si applica al trattamento dei dati personali di persone decedute o di persone giuridiche.

Non rientrano nel regolamento neppure i dati trattati per motivi strettamente personali o per attività svolte in casa a condizione che non vi sia alcun legame con attività professionali o commerciali.

L’accountability

Il GDPR si fonda sul “**principio dell’accountability**“.

Tale termine significa letteralmente “**rendicontazione**” e si riferisce alla responsabilità che incombe sul titolare del trattamento il quale in qualunque momento deve essere in grado di dimostrare (cioè “dare conto”) di avere rispettato il GDPR.

Infatti, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento. Se possiedi un sito web e tratti dati personali devi dimostrare di essere stato responsabile e cioè di avere rispettato il principio dell’”accountability”.

È questo il vero obiettivo principale del regolamento europeo: se riesci a dimostrare la tua “accountability” eviterai certamente il rischio di sanzioni.

A tal fine dovrai svolgere una serie di attività; ad esempio la nomina del **DPO** nei casi in cui è previsto, l’adozione di misure di sicurezza per la protezione dei dati (antivirus, misure di salvataggio dei dati, ecc.).

Molto probabilmente il tuo sito rispetta questi requisiti ma come farai a dimostrarlo se il Garante decide di effettuare dei controlli?

Per questo motivo **devi essere in grado di produrre la documentazione necessaria** in cui spieghi il perché delle tue scelte, in cui valuti i rischi ed in cui adotti le opportune soluzioni.

Tale impegno è valutato in modo positivo dal Garante della privacy, e riduce al minimo il rischio di sanzione.

Che cos'è il Codice della Privacy

Il **codice della privacy** è stato emanato nel nostro Paese con il Decreto legislativo del 2003, n. 196 e ha sempre rappresentato il principale documento giuridico in materia di trattamento dei dati personali.

Tuttavia dopo l'entrata in vigore del GDPR a partire dal 25 maggio 2018, è stato necessario modificare alcune disposizioni del codice della Privacy in contrasto con il regolamento europeo.

A tale proposito è stato emanato il **Decreto legislativo del 2018, n. 101** che ha profondamente modificato il vecchio testo del codice della privacy, armonizzandolo alla nuova normativa.

Rapporto tra GDPR e Codice Privacy

Il GDPR non ha sostituito il codice della privacy ma lo ha integrato e modificato.

Pertanto, in materia di trattamento dei dati personali nel nostro Paese è necessario rispettare sia le norme del GDPR, in quanto direttamente applicabili, sia quelle del Codice della Privacy recentemente modificato dal D.lgs 2018 n. 101.

Che cosa significa trattamento dei dati

Per "trattamento dei dati personali" si intende qualsiasi operazione (o insieme di operazioni) avente ad oggetto i dati personali.

Il GDPR contiene un elenco molto esaustivo di attività che possono coinvolgere i dati personali:

- *la raccolta;*
- *la registrazione;*
- *l'organizzazione;*
- *la strutturazione;*
- *la conservazione;*
- *l'adattamento o la modifica;*
- *l'estrazione;*
- *la consultazione;*
- *l'uso;*
- *la comunicazione mediante trasmissione;*
- *diffusione o qualsiasi altra forma di messa a disposizione;*
- *il raffronto o l'interconnessione;*
- *la limitazione;*
- *la cancellazione o la distruzione.*

Queste operazioni possono essere effettuate **con o senza l'utilizzo di strumenti informatici**.

Pertanto se svolgi delle campagne pubblicitarie per conto di un tuo cliente, stai trattando i dati personali di tutti i soggetti coinvolti nell'attività di marketing. In questo caso ricorda che tu sei il responsabile del trattamento; mentre il titolare del trattamento rimane il tuo cliente.

Se invece esegui delle campagne pubblicitarie per il tuo sito allora sei tu il titolare del trattamento.

Che cos'è la base giuridica

Per "**base giuridica**" si intende l'insieme delle condizioni grazie alle quali il trattamento dei dati personali può essere considerato lecito.

Il GDPR indica quali sono tali condizioni e quali caratteristiche devono presentare (articolo 13 del GDPR).
Le basi giuridiche individuate dal Regolamento europeo sono:

- Il **consenso dell'interessato** che autorizza il trattamento dei dati personali.
- L' **adempimento di un obbligo contrattuale** quando il trattamento dei dati è necessario per l'esecuzione di un contratto.
- L'**adempimento di un obbligo di legge** quando il trattamento dei dati è necessario per rispettare un

adempimento imposto dalla legge (ad esempio l'obbligo per le banche di segnalare i cattivi pagatori alla Centrale Rischi)

- La **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica (ad esempio è necessario chiamare l'autoambulanza per salvare la vita di una persona e comunicare i suoi dati personali).
- La **presenza di un interesse legittimo del titolare del trattamento o di terzi.** In questo caso occorre fare un bilanciamento tra diritto dell'interessato ed interesse legittimo del titolare del trattamento (ad esempio se un cliente ottiene un prestito da una finanziaria e successivamente non paga, la finanziaria ha il legittimo interesse di conoscere il nuovo indirizzo del debitore anche senza il suo consenso).
- La **presenza di un interesse pubblico o connesso all' esercizio di pubblici poteri**. La finalità in questo caso deve essere specificata per legge (ad esempio il trattamento dei dati personali effettuato all'interno delle istituzioni scolastiche).

Se gestisci un sito web la base giuridica che ti riguarda più da vicino è "il consenso" dell'interessato al trattamento dei suoi dati personali.

Per rispettare il GDPR dovrai fare 2 cose:

- **acquisire il consenso dei soggetti coinvolti nella tua attività di marketing**;
- **dimostrare in qualsiasi momento di avere acquisito tale consenso rispettando le regole del GDPR.**

Come dovrebbe essere espresso il consenso

Chiunque tratta dei dati personali prima di compiere qualsiasi attività deve ottenere il consenso dell'interessato. **Per consenso si intende qualsiasi manifestazione di volontà con cui l'interessato esprime il proprio assenso al trattamento dei dati personali che lo riguardano.**

Il GDPR (art. 4) individua le caratteristiche che deve avere tale manifestazione di volontà ed è molto rigido su questo punto. La dichiarazione con cui l'interessato esprime il suo consenso deve essere:

- **libera**: l'interessato non deve subire costrizioni;
- **specifica**: l'interessato deve prestare il suo consenso per ogni singola attività avente ad oggetto i suoi dati personali e per ogni singola finalità perseguita.

Devi stare molto attento a questo aspetto perché se il trattamento ha più finalità, il consenso deve essere prestato per ognuna di esse. Ad esempio se sul tuo sito richiedi sia l'iscrizione alla newsletter sia l'iscrizione ad un videocorso devi ottenere dall'interessato due consensi separati perché si tratta di attività che perseguono finalità diverse.

Inoltre ricorda che se il consenso dell'interessato è richiesto attraverso mezzi elettronici (form di contatto, iscrizione a

newsletter, form per scaricare guide gratuite) la richiesta deve essere chiara, concisa e inoltre:

- **informata**: l'interessato deve conoscere alcune informazioni necessarie affinché tu possa acquisire un valido consenso (la c.d. informativa). Infatti **è preferibile inserire sul sito due check box separati**; uno con cui l'utente dichiara che di aver letto la policy privacy (l'informativa) ed un altro con cui autorizza il trattamento dei suoi dati. Tuttavia se usi le parole giuste puoi inserire un solo check box.
- **inequivocabile**: l'interessato deve esprimere una dichiarazione orale o scritta, svolta anche per via elettronica oppure compiere un'azione attiva, concludente. Di conseguenza, l'inattività e il silenzio non sono sufficienti per esprimere un valido consenso. A tale proposito ricorda che **non costituiscono manifestazione del consenso i form precompilati o le caselle già prespuntate**. In questo ultimo caso, peraltro, il consenso non sarebbe considerato come reso in maniera **libera**.

Dopo avere ottenuto il consenso dell'interessato devi essere in grado in qualsiasi momento di dimostrare al Garante della privacy di averlo attenuto (c.d. **consenso verificabile**).

Il GDPR stabilisce che chi acquisisce il consenso al trattamento dei dati personali (**il titolare del trattamento**) deve essere in grado di dimostrare l'avvenuta acquisizione. Per tale motivo è importante integrare un sistema di tracciamento dei check box.

I soggetti nel GDPR

Soffermiamoci adesso a definire i vari soggetti interessati nel GDPR.

Chi è il titolare del trattamento?

Il Titolare del trattamento (*data controller*) è colui che determina le finalità e i mezzi del trattamento dei dati personali.

Il titolare del trattamento è la persona che **decide come e perché devono essere trattati i dati** (non riceve istruzioni da nessuno).

Sul titolare del trattamento **incombono tutti gli obblighi previsti dal GDPR e le relative responsabilità**.

In particolare gli obblighi del titolare del trattamento sono:

- *adozione delle misure tecniche e organizzative adeguate per garantire, la tutela dei diritti dell'interessato;*
- *dovere di riservatezza dei dati, inteso come dovere di non utilizzare, comunicare o diffondere i dati al di fuori del trattamento;*
- *designazione del responsabile del trattamento;*
- *redazione del registro delle attività di trattamento;*
- *formazione del personale;*
- *inviare comunicazioni al Garante nei casi previsti (violazione dei dati personali o anche "data breach").*

Nel settore privato il titolare del trattamento può essere una persona fisica oppure una persona giuridica.

È possibile che coesistano più titolari del trattamento (contitolari o **jointes controllers**) che decidono congiuntamente di trattare i dati per una finalità comune; ognuno avrà i suoi compiti e le sue responsabilità indicati in un apposito atto scritto.

Quindi se il sito web che gestisci è di tua proprietà, e sei tu a prendere tutte le decisioni relative all'attività di marketing e alla profilazione degli utenti, sarai tu il titolare del trattamento.

Chi è il responsabile del trattamento?

Il responsabile del trattamento (data processor) è colui che elabora i dati personali per conto del titolare del trattamento.

Si tratta di un soggetto distinto dal titolare che deve essere in grado di garantire il rispetto delle norme della privacy in termini di conoscenza specialistica ed affidabilità.

I principali obblighi del responsabile del trattamento sono:

- *garantire la sicurezza e riservatezza dei dati;*
- *avvisare il titolare in caso di violazione dei dati personali;*
- *redazione del registro delle attività di trattamento;*
- *dovere di riservatezza dei dati, inteso come dovere di non utilizzare, comunicare o diffondere i dati al di fuori del trattamento.*

Il titolare del trattamento risponde della gestione effettuata dal responsabile.

Ad esempio sono responsabili del trattamento i tuoi collaboratori che gestiscono per conto tuo le campagne pubblicitarie o le attività di email marketing.

Chi è il DPO?

Il DPO ("*Data Protection Officer*" – Responsabile della protezione dei dati) è una figura introdotta dal GDPR per garantire l'effettivo rispetto delle regole in materia di trattamento dei dai personali (art 37).

Il DPO, infatti, svolge il ruolo di supervisore in tema di privacy e rappresenta un punto di riferimento per il titolare ed il responsabile del trattamento.

Il GDPR prevede che il DPO abbia determinate qualità professionali e capacità; in particolare *deve avere una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati nonché delle norme e delle procedure amministrative che caratterizzano il settore.*

Il DPO può essere un soggetto sia interno che esterno all'organizzazione aziendale, può essere un dipendente del titolare o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. Il titolare del trattamento deve tenere in considerazione 4 aspetti fondamentali per la nomina del DPO:

- **preparazione specialistica**: il DPO deve avere competenza in materia di tutela della privacy;
- **esperienza**: il DPO deve avere abilità e capacità acquisite grazie all'esperienza sul campo; in particolare si richiedono abilità informatiche e di problem solving;
- **aggiornamento**: il DPO deve svolgere una formazione continua, poiché si tratta di una materia flessibile oggetto di una costante evoluzione;
- **imparzialità**: il DPO non deve trovarsi in una situazione di conflitto di interesse ma deve essere una figura indipendente al di sopra delle parti.

La nomina del DPO richiede lo svolgimento di 2 attività fondamentali:

- redazione di un atto di nomina del DPO;
- comunicazione del nominativo del DPO al Garante della Privacy attraverso una specifica procedura.

Il Registro delle attività di trattamento

Il Registro delle attività di trattamento è un documento che contiene le principali informazioni su come vengono trattati i dati personali da parte del titolare.

Tale documento rappresenta uno dei principali strumenti attraverso il quale il titolare rispetta il principio dell'accountability previsto dal GDPR; attraverso il registro, infatti, viene fornito un

quadro aggiornato dei trattamenti posti in essere all'interno della propria organizzazione.

Il documento deve avere la forma scritta, anche elettronica, e deve essere esibito su richiesta del Garante della Privacy e/o delle autorità che svolgono le attività di controllo.

Il contenuto del Registro delle attività di trattamento è indicato dallo stesso GDPR (art. 4). In particolare tale documento deve contenere:

- *il nome e i dati di contatto del titolare del trattamento;*
- *le finalità del trattamento (ad esempio il trattamento dei dati per fornire una consulenza oppure per l'invio di contenuti di testo, audio, video su temi riguardanti i servizi offerti all'interno del proprio sito web);*
- *la descrizione delle categorie di interessati e (ad esempio società, professionisti o privati);*
- *la descrizione delle categorie di dati personali (ad esempio email o numero di telefono);*
- *le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi (ad esempio personale interno o professionisti esterni);*
- *se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione (qualora ciò non avvenga deve essere specificato);*
- *i termini ultimi previsti per la cancellazione delle diverse categorie di dati (è sempre meglio indicare in modo specifico il*

periodo temporale di riferimento ad esempio 6 mesi o 4 mesi a seconda delle finalità perseguite dal titolare);

- *una descrizione generale delle misure di sicurezza tecniche e organizzative (ad esempio gli strumenti di lavoro utilizzati, i sistemi operativi adoperati).*

Anche in capo al responsabile del trattamento sussiste l'obbligo di tenuta di un registro in cui verranno censite tutte le attività di trattamento svolte per conto di un titolare del trattamento.

Che cos'è la DPIA?

La DPIA ("Data Protection Impact Assessment" o "Valutazione d'Impatto sulla Protezione dei Dati") è un documento attraverso il quale il titolare effettua l'analisi dei rischi derivanti dai trattamenti posti in essere.

La DPIA contiene:

- una valutazione delle conseguenze derivanti dal trattamento dei dati sulle libertà e sui diritti degli interessati;
- l'individuazione delle misure necessarie per ridurre l'eventuale rischio.

Il titolare, insieme al responsabile del trattamento, deve effettuare tale valutazione prima di iniziare il trattamento dei dati (valutazione preventiva).

Inoltre egli deve consultarsi col DPO sulla necessità di redazione del documento; il DPO a sua volta ha il compito di fornire, se

richiesto, un parere in merito alla valutazione di impatto e sorvegliarne lo svolgimento.

Nel caso in cui il titolare non concordi con le indicazioni del DPO dovrà motivare e documentare il suo dissenso.

Il contenuto della **DPIA** è indicato nel GDPR; in particolare il documento deve contenere:

- *una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento,*
- *una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*
- *una valutazione dei rischi per i diritti e le libertà degli interessati;*
- *le misure previste per affrontare i rischi.*

Chi deve redigere i documenti previsti dal GDPR (Registro delle attività di trattamento e DPIA)?

La responsabilità di **redazione della DPIA** e del Registro delle attività di trattamento spetta al titolare.

La redazione di tali documenti deve essere effettuata dal titolare insieme al responsabile delle attività di trattamento. Sia la DPIA che il Registro devono essere firmati da entrambi.

Nella redazione di tali documenti il titolare ed il responsabile possono farsi assistere da soggetti interni o esterni all'organizzazione e che siano professionisti del settore (ad

esempio esperti in diritto della privacy, responsabile della sicurezza dei sistemi informativi e del responsabile IT).

Ogni quanto tempo bisogna aggiornare i documenti previsti dal GDPR?

Il GDPR non indica un periodo di tempo specifico decorso il quale il Registro delle attività di trattamento o la DPIA devono essere aggiornati.

Il Regolamento europeo stabilisce però che è necessario effettuare attività periodiche di aggiornamento del Registro e delle misure adottate (art. 24).

Il registro deve essere mantenuto costantemente aggiornato poichè il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere.

Qualsiasi cambiamento in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il registro infatti deve recare "*in maniera verificabile*" sia la data della sua prima istituzione sia la data dell'ultimo aggiornamento.

La stessa cosa vale per la DPIA che deve essere aggiornata quando vengono modificate le misure di sicurezza adottate, i processi di gestione, i software utilizzati.

Pertanto se sei il titolare del trattamento devi effettuare verifiche periodiche sui trattamenti eseguiti (privacy by default).
Inoltre **devi dimostrare di avere svolto l'attività di**

aggiornamento conservando le evidenze dell'attività eseguite, i documenti utilizzati, i piani di adeguamento in corso.

Il diritto della portabilità dei dati

Il GDPR riconosce un nuovo diritto in capo al soggetto interessato: **il diritto alla portabilità dei dati** (art. 20).

In base a questo diritto l'interessato può chiedere al titolare del trattamento che i dati a lui forniti siano trasmessi, senza impedimenti, o a sé stesso o ad altro titolare da lui indicato.

Il Regolamento europeo riconoscendo questo diritto persegue 2 finalità:

- *aumentare il controllo dell'interessato sui suoi dati personali;*
- *facilitare la circolazione dei dati all'interno dell'Unione Europea.*

Il GDPR prevede che, su richiesta dell'interessato, il titolare deve trasmettere i dati attraverso un formato strutturato, di uso comune e leggibile da un dispositivo automatico. Questo significa che **i dati non possono essere trasmessi tramite supporto cartaceo**.

Ogni interessato può esercitare il diritto alla portabilità dei dati in presenza di 2 condizioni:

- *l'interessato deve aver espresso in precedenza il suo consenso al trattamento dei dati personali;*

- *il trattamento dei dati deve essere effettuato con mezzi automatizzati. Sono esclusi quindi i dati conservati in archivi ed elenchi cartacei.*

Pertanto, se sei il titolare del trattamento, su richiesta dell'interessato devi attivarti per garantire l'esercizio di questo suo diritto. In particolare devi compiere queste attività:

- devi informare gli interessati dell'esistenza del diritto in questione;
- devi rispondere alla richiesta dell'interessato in tempi ragionevoli;
- devi adottare modalità che favoriscano la trasmissione dei dati. Ad esempio, devi dare all'interessato la possibilità di scaricarli o di trasferirli direttamente ad un altro titolare utilizzando messaggistica e server sicuri.

La sicurezza del trattamento

Il GDPR introduce l'obbligo per il titolare del trattamento di **mettere in atto misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali** (art. 32).

A tal fine **il titolare deve trattare i dati personali in modo sicuro senza ledere il diritto alla privacy degli interessati**.

Il GDPR prevede che il titolare del trattamento non ha soltanto un obbligo di custodia dei dati personali, ma deve anche adoperarsi per evitare che essi vadano persi o distrutti o violati (art. 5 e art 32

GDPR). In particolare il GDPR suggerisce 3 strumenti che il titolare del trattamento deve utilizzare:

- la **pseudonimizzazione** e la cifratura dei dati personali;
- l'**utilizzo di strumenti che assicurano la riservatezza, l'integrità, la disponibilità, la resilienza dei sistemi** e dei servizi di trattamento (Procedure e programmi di backup, strumenti di analisi dei log e di monitoraggio dei sistemi di ripartenza o recovery);
- l'**utilizzo di strumenti che consentono di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali** in caso di incidente fisico o tecnico (il recupero dei dati salvati – più o meno quello che viene garantito da programmi come Dropbox).

Quindi se sei il titolare del trattamento devi controllare che non ci siano lacune all'interno della tua organizzazione e devi adoperarti concretamente per tutelare i dati personali degli interessati.

Ricorda, inoltre, che devi indicare le misure di sicurezza adottate sia all'interno del Registro delle attività di trattamento, sia all'interno della DPIA e ogni volta che utilizzi un programma o software diverso devi aggiornare tali documenti.

Che cos'è la pseudonimizzazione?

La pseudonimizzazione o cifratura è una tecnica che permette di conservare i dati personali senza identificare il soggetto cui essi si riferiscono.

Per identificare tale soggetto è necessario utilizzare informazioni aggiuntive che devono essere conservate separatamente utilizzando specifiche misure tecniche e organizzative.

Tali misure devono garantire che i dati personali **non siano attribuiti a una persona fisica identificata o identificabile**. In pratica, il titolare deve conservare le informazioni di identificazione (ed eventualmente di profilazione) in maniera tale che non siano riconducibili a una ben precisa persona.

Ad esempio il titolare può utilizzare un **sistema crittografato** mediante l'impiego di una chiave d'accesso; in questo modo, le informazioni contenute in quel file saranno mascherate, protette e lette solo dalle persone che avranno a disposizione la **chiave d'accesso**.

Inoltre le 2 principali tecniche di pseudonimizzazione sono:

- il **Data Masking**: è una tecnica che consiste nel **nascondere i dati personali originali con dati fittizi** (ad esempio può prevedere la sostituzione dei dati con dati simili, la sostituzione dei dati con dati casuali o il rimescolamento dei dati fra loro). I dati devono rimanere validi alla fine dei cicli di test e devono sempre essere utili e fruibili per le attività necessarie allo sviluppo del business del titolare.
- l'**aggregazione**: è una tecnica che permette di **inserire il singolo individuo all'interno di un cluster anonimizzato**. In questo modo il titolare impedisce l'identificazione del soggetto, ma può comunque effettuare operazioni di profilazione e di individuazione di gruppi/target estesi.

> Quindi se sei il titolare del trattamento, e decidi di usare la tecnica della “pseudonimizzazione” dei dati, riuscirai a proteggere i dati dei tuoi clienti in modo **conforme alle norme del GDPR**.

Responsabilità in caso di violazione dei dati personali.

L’unico responsabile nel caso in cui non vengano rispettate le disposizioni del GDPR è il titolare del trattamento.

Il principio dell’accountability pone tale figura al centro di tutta la normativa; infatti è il titolare a decidere le modalità e le finalità del trattamento a mettere in atto le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (art 24).

La responsabilità di garantire il rispetto del GDPR ricade quindi solo sul titolare del trattamento o sul responsabile del trattamento (art. 82). Il responsabile, infatti, risponde per il danno causato dal trattamento solo in caso di non corretto adempimento dei suoi obblighi oppure se ha agito in modo difforme rispetto alle istruzioni del titolare del trattamento.

Il considerando n. 28 prevede in capo al responsabile un dovere di verifica e controllo generale con conseguente responsabilità, in solido col titolare, nelle ipotesi di omesso controllo o omessa informazione.

Il DPO invece è responsabile in caso di violazione dei suoi obblighi di consulenza e assistenza solo nei confronti del titolare del trattamento.

Le violazioni poste in essere dal DPO possono essere di 2 tipi:

- **contrattuali**: il titolare del trattamento può richiedere il risarcimento del danno al DPO se lo stesso DPO è un soggetto esterno;
- **contrattuali e/o disciplinari**: se il DPO è un dipendente o collaboratore del titolare del trattamento quest'ultimo può adottare delle sanzioni disciplinari (interne all'azienda).

In ogni caso il titolare del trattamento rimane l'unico soggetto responsabile del rispetto della normativa vigente.

Quindi se gestisci un sito web e sei il titolare del trattamento sarai tu a rispondere di fronte al Garante della Privacy.

Questo succede anche se la violazione è stata commessa per colpa del DPO; successivamente potrai eventualmente agire nei suoi confronti a causa del danno subito (a condizione che il DPO abbia effettivamente contribuito a causare il danno).

Comitato Europeo per la Protezione dei Dati: cos'è?

Il **Comitato Europeo per la Protezione dei Dati** (*EDPB – European Data Protection Board*) è un organismo indipendente che fornisce pareri e chiarimenti in materia di **tutela della Privacy**; il

suo intervento è costante ed avviene attraverso la pubblicazione di Linee guida che tutti i titolari e responsabili del trattamento devono rispettare.

Il Comitato Europeo per la Protezione dei Dati ha sostituito il famoso "Gruppo di Lavoro ex art. 29" della Direttiva 95/46 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Tale Direttiva è stata abrogata dal GDPR.

Le Linee Guida del Comitato Europeo per la Protezione dei Dati (ex Gruppo di Lavoro art 29) sono state tradotte in tutte le lingue europee; una corretta applicazione del GDPR, quindi, richiede sia il rispetto delle norme in esso contenute sia l'osservanza delle Linee Guida.

Comitato Europeo per la Protezione dei Dati: perché deve interessarti?

Il Comitato Europeo per la Protezione dei Dati (che ha sostituito il famoso "Gruppo di Lavoro ex art. 29") viene spesso citato per risolvere alcuni dubbi interpretativi sul diritto della privacy.

In buona sostanza, **se il GDPR contiene delle norme vaghe e lacunose, molto probabilmente la risposta sarà contenuta in alcuni pareri espressi dal Comitato**.

Come gestore di un sito web è importante che tu conosca l'esistenza di questo organo: alcune decisioni del Garante della

Privacy si fondano sui pareri espressi dal Comitato, che risolvono i dubbi interpretativi più significativi contenuti nel GDPR.

Privacy Policy: che cos'è

La "**Privacy Policy**" spesso anche definita "**Informativa sulla Privacy**" è un documento che informa gli utenti di un sito web, ad esempio, su come il titolare del trattamento userà i loro dati personali.

L'articolo 13 del GDPR prevede che in caso di raccolta di dati personali, il titolare del trattamento deve fornire all'interessato le seguenti informazioni:

1. *l'identità e i dati di contatto del titolare del trattamento;*
2. *i dati di contatto del responsabile della protezione dei dati (DPO), ove applicabile;*
3. *le finalità del trattamento nonché la base giuridica del trattamento;*
4. *il periodo di conservazione dei dati personali;*
5. *l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi.*

Pertanto se gestisci un sito web, un software o una "mobile app", devi predisporre una Privacy Policy che contenga tutte le informazioni prescritte dall'articolo 13 del GDPR; l'informativa avrà lo scopo di informare i tuoi visitatori su come utilizzerai i loro dati.

Uno degli errori più comuni quando si predispone una Privacy Policy è quello di **utilizzare risorse gratuite**; tale scelta può rivelarsi molto rischiosa perché non fornisce un servizio completo.

Infatti **tutte le risorse gratuite sul web consentono la creazione di un'informativa incompleta** senza l'inserimento di tutte le informazioni richieste dall'art. 13 del GDPR.

Allo stesso modo copiare la Policy presente su un altro sito e adattarla al tuo caso può essere una soluzione molto pericolosa; infatti il documento che userai come template è stato creato per regolare una realtà imprenditoriale diversa dalla tua e descriverà attività di trattamento dei dati differenti da quelle che persegue la tua azienda.

Per redigere una Privacy Policy perfetta dovrai seguire le indicazioni prescritte dall'art. 13 del GDPR; la tua policy dovrà contenere:

1. *Tutti i riferimenti normativi richiesti dal GDPR* (per questa attività hai bisogno di un legale);
2. *Tutte le finalità di trattamento che stai perseguendo* (per quest'attività è necessario effettuare un'indagine completa);
3. *Tutte le attività di marketing e profilazione che stai eseguendo* (per quest'attività è necessario comprendere la tua strategia di comunicazione sul web).

I diritti degli interessati

Uno degli adempimenti più importanti del GDPR è quello di informare gli utenti di un sito web su quali siano i loro diritti.

Pertanto nella Privacy Policy sarà obbligatorio indicare tutte le azioni e le attività che l'interessato potrà esercitare a difesa dei propri dati personali (come la **portabilità del dato**, il **diritto alla cancellazione** o il **diritto all'oblio**).

Fin troppe policy sul web non contengono alcuna informazione su questo punto: si tratta di una grave lacuna che può essere sanzionata dal Garante.

Cookie Policy – Cos'è

La **Cookie Policy** è un'informativa che descrive in modo dettagliato le **regole di tracciamento dei cookies** che esegui con il tuo sito web.

In base a quanto prevede la legge, ogni sito web deve possedere un documento che informi i visitatori sulla politica di tracciamento dei cookies.

Cosa sono i cookies?

I cookies sono delle informazioni (sotto la forma di codice web) **che un server può inviare ad un dispositivo elettronico**

connesso alla rete (pc, smartphone o tablet); l'informazione (cioè il cookie) viene inviata dal server quando:

- un determinato utente visita un sito web;
- lo stesso utente acconsente al tracciamento del cookie.

Facciamo un esempio concreto: Giorgio (un utente) visita un sito web che parla di marketing; durante la navigazione Giorgio vede apparire una finestra "pop up" che gli chiede di autorizzare il tracciamento dei cookies.

Giorgio clicca sul bottone collocato sulla finestra "pop up" autorizzando il tracciamento dei cookies. Di solito dopo il click, la pagina web viene ricaricata e il server (su cui è hostato il sito web) invia i cookies (sotto forma di codice) nel browser usato da Giorgio.

In una fase successiva, lo stesso server che ha trasmesso i cookies, può leggere e registrare quei frammenti di codice (i cookies appunto) che si trovano sul dispositivo elettronico di Giorgio (pc, smartphone o tablet) per ottenere informazioni di vario tipo.

I cookies possono avere funzioni diverse: in molti casi sono utili perché **rendono più semplice e veloce la navigazione** (come accade con i **cookies tecnici** – utilizzati per esempio per salvare le preferenze di lingua o un carrello della spesa).

In altri casi, invece, i cookies sono utilizzati per **monitorare gli utenti durante la navigazione**; i cosiddetti "**cookies di profilazione**" che registrano informazioni su ciò che compri o

potresti voler comprare, analizzando le tue letture, i tuoi hobby e le tue preferenze di acquisto.

Esistono infine i "**cookies di terze parti**", ovvero quelle informazioni che vengono registrate da siti diversi rispetto a quelli che hai visitato; i "cookies di terze parti" vengono utilizzati a **scopi di profilazione**.

Piccoli accorgimenti tecnici

Non è necessario che la "Cookie Policy" sia inserita in una pagina web separata; è sufficiente che tu informi gli utenti sulla politica di tracciamento dei cookie del tuo sito web creando un'apposita sezione dedicata a questo tema nella tua "Privacy Policy".

Peraltro la creazione di un unico documento, che contenga sia l'informativa sulla privacy sia l'informativa sui cookie, può essere una scelta più gradita dall'autorità di controllo poiché permette agli utenti di un sito web di acquisire tutte le informazioni di trattamento dei dati in un'unica pagina, migliorando pertanto la "user experience" per tutti i visitatori e la facilità di accesso alle informazioni.

Il Garante per la protezione dei dati personali ha adottato in data 10 giugno 2021 le "**Linee guida cookie e altri strumenti di tracciamento**" con l'obiettivo di specificare ulteriormente e aggiornare le corrette modalità per la fornitura dell'informativa e per l'acquisizione del consenso on-line degli utenti nel rispetto della complessa normativa privacy. In particolare, il Garante ha

fornito alcuni chiarimenti e raccomandazioni che si possono riassumere per punti, come segue.

- **scrolling e cookie wall**: il semplice "scroll down" del cursore di pagina non è una modalità valida per l'acquisizione del consenso, non potendo essere considerato quale azione positiva e inequivocabile dell'interessato. Stesse considerazioni valgono per il cookie wall poiché lo stesso rappresenta un obbligo per l'utente ad esprimere il proprio consenso al tracciamento, pena l'impossibilità di accedere, visualizzare e navigare sul sito;
- **reiterata richiesta del consenso**: il gestore di un sito web non può e non deve ripresentare il banner dei cookies all'utente ad ogni suo nuovo accesso al sito quando l'utente, in precedenza, ha già liberamente scelto di non prestare il proprio consenso o prestarlo in relazione a determinate categorie di cookies (sarà possibile farlo solo nel caso in cui siano mutate significativamente le condizioni del trattamento);
- **corretta impostazione dello strumento di gestione dei cookies**: al momento del primo accesso da parte dell'utente sul sito web, per impostazione predefinita, nessun cookie che non sia tecnico potrà essere posizionato all'interno del dispositivo dell'utente, né potrà essere utilizzata alcuna tecnica di tracciamento. Ciò sarà possibile solo in una fase successiva all'eventuale consenso reso dall'utente;
- **aspetto grafico del banner**: le dimensioni del banner devono essere discrete, tali da non impedire all'utente la fruizione dei contenuti presenti sul sito web. Il banner, inoltre, dovrebbe

presentare i tre pulsanti “accetta tutti”, “personalizza”, “rifiuta tutti” (o eventualmente una “X” ben visibile posizionata nell’angolo in alto a destra del banner”), i quali dovranno essere simili per forme, dimensioni e colori utilizzati. Il banner dovrà, inoltre, contenere all’interno del suo testo: un’informativa minima rispetto ai cookies utilizzati, il link alla privacy policy estesa, l’avvertenza che in caso di rifiuto si potrà continuare la navigazione del sito in assenza di cookie diversi da quelli tecnici.

Si ricorda, infine, che nel rispetto del principio di responsabilizzazione del titolare del trattamento, dovranno essere predisposti congrui strumenti, informatici e non, in grado di gestire il salvataggio dei consensi espressi dagli utenti. È onere del titolare del trattamento, infatti, dimostrare di aver ottenuto il consenso dell’interessato per il perseguimento di una determinata finalità e ciò vale anche con riferimento ai consensi resi dagli utenti nell’ambito del banner dei cookies.

L’attività di marketing per il GDPR

Per lavoro e per deformazione professionale, abbiamo analizzato moltissime privacy policy presenti sul web e abbiamo notato una tendenza frequente: moltissime informative non contengono una descrizione molto specifica sulle attività di marketing svolte dai titolari di trattamento.

Questa pessima abitudine è certamente causata da numerosi fattori: copia e incolla di policy incomplete, utilizzo di software gratuiti, mancata conoscenza della normativa sulla privacy.

Una buona privacy policy deve necessariamente informare tutti i visitatori sulle attività di marketing svolte dal titolare del trattamento.

Se il tuo sito web svolge campagne pubblicitarie sui Social, gli utenti dovranno essere informati su come userai i loro dati; analogamente se svolgi attività di lead generation tutti gli utenti che si iscrivono alla tua newsletter dovranno sapere come gestirai i loro dati personali.

L'attività di profilazione nel GDPR

In numerosi articoli del GDPR si utilizza la parola "**profilazione**"; senza scendere in definizioni tecniche e astratte, con tale termine si identificano **tutte le attività svolte dal titolare del trattamento per misurare le performance delle campagne di marketing.**

In poche parole: se svolgi campagne di paid advertising l'attività di profilazione consisterà nella misurazione del rendimento della campagna.

Facciamo un esempio concreto: Mauro (un freelancer) svolge campagne di lead generation su Facebook per acquisire lead per il suo sito di modellismo. Una volta terminata la campagna su Facebook, Mario analizzerà tramite il Business Manager i risultati della sua attività e verificherà quante persone hanno mostrato interesse per la sua inserzione. In questo caso il freelancer scoprirà che gli uomini compresi tra i 35 ed 45 anni, che si trovano nella regione del Lazio, sono più interessati ai suoi prodotti. Ecco

l’analisi dei dati eseguita da Mario deve essere qualificata come “attività di profilazione”.

Cosa significa tutto questo?

Devi sapere che **se svolgi attività di profilazione** (e dunque se misuri il rendimento delle tue campagne di marketing) **il GDPR prevede l’obbligo di nominare un DPO** (Data Protection Officer) ovvero un Responsabile della Protezione dei dati, a patto che siano presenti alcune condizioni.

Quali sono le condizioni per cui il GDPR prevede l’obbligo di nomina del DPO?

Come già descritto in precedenza, l’art. 37 del GDPR prevede che

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta … le attività principali del titolare del trattamento consistono in trattamenti che … richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

In questa controversa norma (criticata aspramente da molti legali e imprenditori) si annidano tutti i pericoli di sanzione per gli operatori del marketing.

In sostanza la nomina del DPO è necessaria:

- **quando si effettua attività di profilazione** (monitoraggio regolare e sistematico degli interessati);

- **quando l’attività di profilazione è eseguita su “larga scala”**.

Questo ultimo termine “larga scala” è certamente l’enigma più misterioso del GDPR.

Cosa si intende per “larga scala”?

Il GDPR non lo dice e non fornisce dei criteri quantificativi e numerici per verificare se l’attività di profilazione è effettuata su larga scala.

Tuttavia la generica formulazione della norma si traduce in un accrescimento del potere discrezionale attribuito al Garante. In altre parole se la norma è generica, allora il suo significato può essere interpretato in modo arbitrario dall’autorità di controllo.

Cosa significa tutto questo in concreto con le attività di marketing?

Ci spieghiamo meglio: se un imprenditore o un freelancer effettua delle campagne di advertising su Facebook su tutta Italia che raccolgono migliaia di lead, potremo certamente affermare che l’attività di profilazione sarà eseguita su “larga scala”.

In questo caso devi nominare il DPO: lo dice il GDPR.

Ma cosa succede se l’attività di profilazione si concentra solo in una regione o addirittura in una sola città? (sappiamo che il Business Manager di Facebook consente questa scelta). In questo

caso l’attività di marketing e di profilazione è eseguita su larga scala?

Non è semplice rispondere, proprio perché non abbiamo dei criteri quantitativi; in ogni caso occorrerà eseguire una valutazione ponderata, misurando i risultati della campagna con i dati demografici dell’area geografica interessata.

Insomma non esiste una risposta precisa a questa domanda. Semmai la risposta può essere fornita direttamente dal Garante della Privacy.

Proprio perché la norma è generica e astratta, nulla impedisce al Garante della Privacy (che ricopre la qualifica di organo di controllo sulle attività di trattamento dei dati) di attribuire un significato più preciso alle due parole “larga scala”.

Tuttavia non è il caso di terrorizzarsi: usando il buon senso e chiedendo il parere di un esperto è possibile rispettare la normativa europea senza correre il rischio di sanzioni.

Il Garante è un organo di controllo che svolge la sua funzione pubblica e che persegue l’interesse generale dello Stato. Ci hanno spesso insegnato ad avere fiducia nelle istituzioni: il nostro consiglio è quello di adottare un comportamento prudente per evitare possibili rischi di violazione del GDPR.

Nel dubbio scegli sempre la soluzione più sicura per i tuoi utenti. Il trattamento di migliaia di dati (lead) è un’attività abbastanza rischiosa.

GDPR: le sanzioni

La violazione delle norme contenute nel GDPR può determinare l'applicazione di sanzioni molto severe. Le multe applicate dalle autorità di controllo dipendono da 3 fattori:

- *la gravità della violazione;*
- *la durata della violazione;*
- *la natura della violazione.*

Dalla combinazione di questi 3 elementi il Garante della Privacy può applicare delle sanzioni amministrative pecuniarie che si dividono in due categorie.

Sanzione N. 1 = 2% del fatturato o sanzione fino a 10 milioni di euro

L'autorità di controllo può applicare alternativamente:

- una sanzione fino a 10 milioni di euro;
- se superiore, una sanzione pari al 2% del fatturato annuo complessivo dell'azienda che ha commesso la violazione;

Il Garante ha il potere di scegliere una delle due sanzioni pecuniarie, accertando quale sia la maggiore, nei seguenti casi:

- nel caso in cui il trasgressore non possa assicurare un **grado idoneo di sicurezza** e non possa dimostrare di aver adottato idonee misure di prevenzione;
- nel caso in cui il trasgressore **non abbia nominato un DPO**;
- nel caso in cui il trasgressore **non abbia raggiunto un accordo nel trattamento dei dati**.

Sanzione N. 2 = 4% del fatturato o sanzione fino a 20 milioni di euro

Quando il trasgressore ha violato i diritti delle persone interessate (come ad esempio nel caso in cui siano trattati dati personali di utenti senza aver acquisito il consenso) l'autorità di controllo può applicare delle sanzioni più rigide:

- una sanzione fino a 20 milioni di euro.
- se superiore, una sanzione pari al 4% del fatturato annuo complessivo dell'azienda che ha commesso la violazione.

Anche in questo caso il Garante ha il potere di scegliere una delle due sanzioni pecuniarie, accertando quale sia la maggiore.

Pertanto se gestisci un sito web e se svolgi attività di lead generation, uno dei pericoli maggiori che potresti correre è quello di **inviare DEM** e messaggi email senza aver acquisito il consenso degli interessati; tale comportamento può causare l'applicazione di una sanzione molto severa.