Modello Organizzativo Privacy Policy web

Sommario

1. INFORMATIVA PRIVACY

L'informativa sulla privacy è, sicuramente, il documento più importante perché da lì si può capire se il Titolare del sito web ha lavorato scrupolosamente o sommariamente, magari "scopiazzando" qua là informative dagli altri siti.
L'informativa ci dice, e ci deve dire, in modo esaustivo, chiaro e trasparente, tutto quello che abbiamo fatto, che facciamo e che faremo con i dati degli utenti, da quelli che semplicemente navigano il sito fino a quelli che con il sito hanno un'interazione maggiore come gli acquirenti on-line o i sottoscrittori di un servizio ad esempio newsletter.
In definitiva con l'informativa rendi note all'utente, fruitore del tuo sito web, le seguenti tipologie di informazioni:

- quali dati raccogli;
- quanti dati raccogli;
- in che modalità tratti i suoi dati;
- per che finalità raccogli i suoi dati;
- se il trattamento è lecito e per quale motivo;
- per quanto tempo conservi i dati;
- come proteggi i suoi dati;
- chi può avere accesso ai dati;
- a chi possono venire comunicati e/o trasferiti i dati;
- come può contattare il Titolare, il suo o i suoi Responsabili e, se nominato, il Responsabile della Protezione Dati o DPO.

Quindi, vediamo quali informazioni deve contenere l'informativa:

- informazioni generali sull'azienda, l'ente pubblico o organizzazione, quindi una descrizione sintetica dell'attività;
- quali tipologie di dati vengono richiesti tramite un eventuale modulo di contatto;
- importantissimo specificare per quali finalità ben distinte vengono utilizzati i dati e se necessitano di un consenso;
- indicare su quali BASI GIURIDICHE poggiano le finalità per cui si raccolgono i dati personali, quali in base a obblighi contrattuali o pre-contrattuali, obblighi di legge, legittimo interesse, pubblico interesse o in base al consenso dell'interessato;
- se esiste un processo di profilazione dei dati in base al quale vengono prese decisioni senza intervento umano;
- indicare i fornitori di terze parti, nominati come Responsabili Esterni del trattamento che trattano i dati dei tuoi utenti e i link alle rispettive pagine privacy;
- link alle rispettive pagine privacy dei fornitori di terze parti che hanno servizi attivi sul sito web mediante cookies con servizi che tengono traccia dei dati degli utenti finali;
- a chi potrebbero essere trasferiti e/o comunicati i dati, ad esempio altri Enti Pubblici, Forze di Polizia, Responsabili esterni ecc.;
- chi per conto del Titolare del trattamento accede ai dati, dipendenti autorizzati interni, collaboratori o Responsabili esterni;
- deve inoltre indicare chiaramente quali sono i diritti dell'interessato e come può esercitarli;
- devono essere presenti i dati di contatto del Titolare del Trattamento e del DPO/RPD (Data Protection Officer o Responsabile Protezione Dati se presente).

L'informativa deve essere BEN VISIBILE ed ACCESSIBILE da ogni parte del sito e in tutte le form di richiesta dati!

2. COOKIE

I cookies sono dei semplici marcatori software che consentono di rilevare dati dell'utente quali indirizzo IP, tipo di dispositivo e browser, posizione geografica, data e ora, comportamenti sul sito, pagine visitate, click e così via…
Alcuni di questi cookies sono installati e gestiti direttamente dal gestore del sito e sono strettamente funzionali per la fruizione del sito stesso, denominati cookie tecnici, o per scopi statistici, denominati cookie analitici, e infine di profilazione. Altri invece sono installati e gestiti da società esterne al sito, denominati di "terze parti", come ad esempio Google Ads, Facebook, Linkedin etc..

Risulta quindi necessario definire nella privacy policy quali cookie vengono utilizzati nel sito e per cosa servono distinti in:

- Cookie tecnici di "navigazione" o di "sessione" e sono quelli strettamente necessari all'uso del sito;
- Cookie Analytics assimilabili a quelli tecnici che rilevano dati statistici in forma aggregata ad esempio il numero di visitatori, orari, area geografica ecc.;
- Cookie di profilazione e sono quelli che permettono di creare un profilo in base ai comportamenti dell'utente sul tuo sito;
- Cookie di profilazione di terze parti e sono installati e gestiti da società terze ad esempio Google Analytics se viene rilevato anche l'indirizzo IP in chiaro.

I soli cookie tecnici e analytics NON necessitano di consenso, ma occorre un semplice banner che contenga un messaggio del tipo: "Questo sito usa solo cookie tecnici strettamente indispensabili alla navigazione, se vuoi sapere quali leggi l'informativa privacy al seguente link".

Riguardo i cookie di profilazione raccolti direttamente dal sito è necessario richiedere un consenso inserendo nello stesso banner una frase che informa della presenza di questa tipologia di cookie con un messaggio del tipo: "Questo sito utilizza cookie per inviarti comunicazioni e servizi in linea con le tue preferenze. Se vuoi saperne di più o negare il consenso a tutti o ad alcuni cookie clicca sul seguente link. Chiudendo questo banner, scorrendo questa pagina o cliccando qualunque suo elemento acconsenti all'uso dei cookie…".

Per i cookie di profilazione di terze parti è necessario chiedere un ulteriore consenso. Se però il sito web utilizza cookie quali ad esempio Google Analytics rendendo anonimo l'indirizzo IP il consenso non risulta necessario.

Il banner relativo alla gestione dei cookie, come disposto dal Garante, deve avere le seguenti caratteristiche:

- dimensioni tali da renderlo facilmente visibile, o espandibile;
- font più evidenti rispetto a quello del sito;
- un colore dello sfondo contrastante rispetto allo sfondo del sito e al testo del banner stesso;
- deve comparire immediatamente alla prima visita dell'utente sul sito.

Il consenso ai cookie può avvenire:

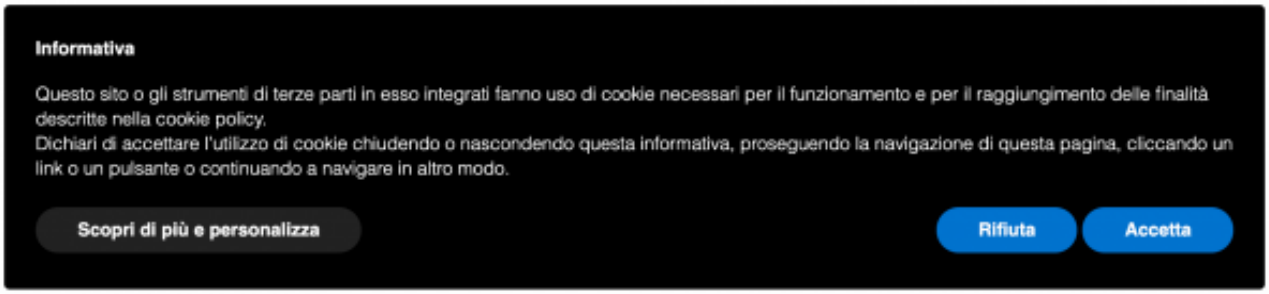
- compiendo un'azione di scorrimento, scroll-down della pagina;
- in alternativa facendo clic su uno dei link interni della pagina;
- in alternativa facendo clic sull'eventuale tasto "OK" o sul tasto "X" di chiusura banner.

L'informativa relativa ai cookie deve essere parte integrante o comunque all'informativa generale e deve contenere:

- una descrizione sintetica di cosa sono i cookie e come possono essere disabilitati tramite le impostazioni del browser;

- la spiegazione di come viene prestato l'eventuale consenso;
- la descrizione delle categorie di cookie tecnici e analytics e relative finalità;
- la descrizione dei cookie di profilazione di prima parte con l'eventuale modulo di consenso;
- la descrizione dei cookie di terza parte e, per ognuno di questi, potenzialmente identificabile anche tramite il nome commerciale, come Facebook, Google ecc., la descrizione della finalità del cookie oltre al link all'informativa e al modulo di consenso della terza parte con la quale si è stipulato un accordo per l'installazione dei cookie sul proprio sito.

Un semplice esempio di banner potrebbe essere come il seguente;



3. MODULI DI RICHIESTA DATI

Particolare attenzione deve essere posta a quelle parti del sito che richiedono dati personali ovvero: moduli di contatto e form di iscrizione a newsletter.
Troppo spesso si vedono form di richiesta dati eccessive, che chiedono troppi dati rispetto alle finalità per cui sono raccolti andando contro ad uno dei principi fondamentali del GDPR quello di "minimizzazione e proporzionalità".
Se per esempio devi scegliere i campi da inserire in una form d'iscrizione alla newsletter puoi chiedere, oltre ovviamente alla mail, il nome e magari anche il cognome o la città e l'azienda, o anche i suoi interessi per personalizzare meglio la comunicazione ma, non sicuramente il telefono perché non servirebbe per raggiungere quella finalità specifica.
Se vuoi avere quindi una form di richiesta dati secondo il Gdpr devi seguire queste 4 regole:

- non eccedere nella richiesta di dati che non siano strettamente necessari al raggiungimento della finalità;
- prevedere sempre una casella di spunta con un link all'informativa privacy ed un messaggio del tipo "Ho letto ed accetto le modalità di trattamento dei dati descritte nella Privacy Policy";
- prevedere una casella di consenso diversa per ogni specifica finalità (ad esempio: una per l'invio di comunicazioni marketing, un'altra per il consenso alla profilazione e magari un'altra per il trasferimento dei dati ad altri Titolari)
- le caselle NON devono essere PRE-SPUNTATE o impostate sul Sì nel caso ci sia l'opzione Si/No.

4. CONSENSO

Se i consensi sono stati ottenuti prima del 25 maggio 2018, data di applicazione del GDPR, non è detto che occorra richiederli nuovamente.
È comunque indispensabile controllare che questi consensi siano stati ottenuti rispettando i principi del GDPR altrimenti bisogna chiedere un nuovo consenso, soprattutto nei casi sottoelencati:

- se c'era un consenso unico che comprendeva più finalità, ad esempio per marketing, profilazione e trasferimento dati personbali a terzi;

- se esistevano le caselle dei consensi pre-spuntate;
- se non si è in grado di dimostrare il consenso;
- se il consenso è datato rispetto alla tipologia di prodotto che tratti.

Per ottenere un nuovo consenso è possibile inviare una mail alla tua lista, specificando che esiste la necessità di confermare i dati forniti in precedenza tramite un bottone, una spunta o qualsiasi altra forma che preveda un'azione libera ed inequivocabile dell'utente per ogni finalità quindi, in breve:

- inviare una mail con la nuova informativa per chiedere conferma dei dati e un nuovo consenso;
- cancellare dalla lista i nominativi che non ti hanno rinnovato il consenso;

5. BACKUP

In caso di incidente informatico, il modo migliore per garantirti di far ripartire velocemente il sito web e di non perdere irrimediabilmente i dati personali ed incorrere inevitabilmente in un Data Breach con conseguente segnalazione al Garante entro 72 ore, è quello di avere sempre a disposizione un BACKUP recente e consistente rispettando questi requisiti:

- il backup meglio se programmato con esecuzione automatica e con schedulazione giornaliera, sia per i contenuti del sito web, quali articoli, pagine e immagini, ma, soprattutto per i database che contengono i dati personali degli utenti;
- meglio assicurarsi di avere più copie dello stesso backup, in più posti diversi, ambiente locale, su un Cloud e offline;
- limitare l'accesso ai dati di backup alle sole persone e/o Responsabili autorizzati o nominati;
- usare supporti, dischi o sistemi che prevedono la cifratura dei dati soprattutto se esistono dati particolari;
- prevedere a livello periodico dei test sul buon fine dei backup, almeno una volta a semestre, con prove di ripristino dei dati atti a verificarne l'integrità e documentare sempre tutte le attività;

6. HOSTING

Il GDPR prevede agli articoli da 44 a 46, che se i dati personali di un interessato residente in Europa vengono trasferiti verso paesi terzi che non forniscono adeguate garanzie di sicurezza e protezione dati è necessario sempre il consenso altrimenti il trattamento è illecito.

Assodato che oramai qualsiasi sito web si avvale di servizi hosting consistenti in spazi server che risiedono presso Datacenter in Cloud sparsi per il mondo bisogna chiedersi DOVE fisicamente stanno questi dati.
La risposta, quando si parla di servizi Cloud, non è così semplice. Per garantire la BUSINESS CONTINUITY e il DISASTER RECOVERY molti fornitori Cloud replicano i dati su DataCenter ridondanti in giro per il mondo e, spesso neanche loro sanno dire con precisione dove sono questi dati.
Se questo da un lato è una garanzia per la salvaguardia del business, dall'altro pone il problema dei dati personali che risiedono in paesi terzi che non hanno normative chiare in merito alla Privacy come ad esempio Russia, Cina ed India.
È meglio quindi affidarsi a fornitori Cloud che dispongono di servizi HOSTING locati in DataCenter all'interno della UE e che lo dichiarano apertamente nelle loro policy.
In ogni caso, se vuoi per forza avvalerti di un servizio Hosting extra UE, devi dichiarare chiaramente la locazione nell'informativa indicando se il paese dove risiedono i dati fornisce

garanzie di adeguatezza e, nel caso non ci siano queste garanzie, chiedere il consenso ai tuoi utenti al trasferimento dei dati in paesi extra Ue.

7. CONCLUDENDO

Il SITO WEB deve essere una PRIORITÀ in un progetto di GDPR compliance perché, oltre a rassicurare gli utenti, quindi i vostri potenziali e futuri clienti, che i dati verranno trattati con la massima attenzione, serve anche dimostrare alle Autorità di Controllo che, potrebbero fare queste analisi con estrema facilità, almeno per quanto riguarda il sito web occorre essere sensibili ed aggiornati in materia di disposizioni e normative privacy evitando quindi di accendere lampadine rosse che potrebbero far scattare ulteriori e più approfondite ispezioni.