Come avere un sito web a prova di GDPR: 5 regole d'oro

Autore: Luisa Di Giacomo
In: Diritto civile e commerciale

Hai un sito internet oppure un e-commerce o stai pensando di aprirne uno, ma non sai come orientarti per essere **compliant al GDPR**, la famigerata normativa per la protezione dei dati personali?

Dopo aver visto mille tutorial e letto innumerevoli articoli si possono avere le idee più confuse di prima, e siccome le multe sono piuttosto salate e **il sito web è la nostra vetrina** nei confronti del mondo, è bene farsi trovare preparati, non solo dal punto di vista estetico, ma anche da quello normativo.

Ecco una **breve guida sulle cinque cose che non devono assolutamente mancare su un sito internet per essere a prova di Garante.**

>> GUARDA il VIDEO della breve guida <<

Indice:

Diritto & Diritti ISSN 1127-8579

1.Il sito deve essere sicuro

La prima regola è che il sito deve essere **sicuro** e quindi deve trasmettere in **protocollo https** e non semplicemente http.

Quella S alla fine vuol dire proprio "**secure**", sicuro. Oltre a non esserci niente di peggio che andare su un sito, specie se aziendale o istituzionale, e leggere sulla barra degli indirizzi "**non sicuro**", si tratta non solo di un problema di immagine, ma anche di **sicurezza nella trasmissione delle informazioni**.

Https vuol dire che i contenuti del tuo sito saranno **criptati**, e soprattutto se si tratta di un e-commerce, i dati dei tuoi clienti, login, password e dati delle disposizioni di pagamento transiteranno su server protetti.

Nessuno si fiderà a lasciare i propri dati su un sito non protetto, figuriamoci la propria carta di credito. Acquistare un **certificato SSL e mantenerlo valido ed aggiornato** avrà una triplice funzione: fornirà una immagine di serietà, proteggerà nella pratica i dati degli utenti ed eviterà che il Garante pensi che si prende sotto gamba la normativa in tema di protezione dei dati, decidendo magari fare una capatina in azienda per effettuare altri controlli.

2.Informativa cookies e banner

Il sito deve essere sottoposto ad una analisi tecnica, e sarà quindi necessario **chiedere al nostro webmaster**, all'agenzia che si è occupata della nostra comunicazione web, a un tecnico, insomma a chi materialmente ha messo le mani nelle nostre pagine ed è **competente per rispondere quali tipi di cookie sono presenti**. E dalla risposta dipenderanno le nostre decisioni.

Della nuova normativa cookies e dei diversi tipi di banner abbiamo già ampiamente parlato **in questo articolo**. Qui basti ricordare che le cookie policy non possono e non devono essere copiate da un sito che ha una attività simile, perché non è detto che i sistemi di tracciamento siano uguali.

Peraltro, con l'anno nuovo entreranno in vigore **le nuove regole**, quindi sarà ancora più stringente il principio di data protection by design e by default, con conseguenti controlli maggiormente stringenti.

Se è necessario ripassare che cosa sono i cookies e come vanno gestiti, **clicca qui per vedere una guida completa sull'argomento.**

Leggi anche:

Diritto & Diritti ISSN 1127-8579

- Cookie e altri strumenti di tracciamento: guida pratica per un banner a prova di GDPR
- Guida alla nuova disciplina sui cookie e altri strumenti di tracciamento

3.Privacy policy

La privacy policy del sito non dovrà essere copiata e dovrà **indicare nello specifico quali dati vengono trattati, non solo quelli di navigazione, ma anche quelli forniti volontariamente,** in caso di presenza di newsletter o moduli di contatto.

La policy deve contenere tutti i requisiti previsti dagli artt. 13 e 14 del GDPR.

Un consiglio di buona prassi è quello di prevedere una **sezione privacy per inserire tutte le informative** (sì, al plurale e no, non è un refuso), ovvero non solo la policy del sito, ma anche l'informativa clienti e fornitori, quella per il trattamento dei curriculum vitae (nel caso il sito abbia una sezione "**lavora con noi**", ma anche in caso di invio spontaneo di candidature) e quelle per trattamenti particolari effettuati (gift card, newsletter, marketing o altro).

In questo modo, non solo il Titolare dimostrerà di essere sempre ben consapevole dei dati trattati, ma gli interessati avranno sempre sotto controllo i propri dati e potranno esprimere le preferenze in piena consapevolezza.

4.La gestione dei consensi

La regola "nel più sta il meno" non vale per i consensi sul trattamento dei dati. Il consenso è una delle basi del trattamento, ma **deve essere richiesto quando serve e solo quando serve,** non a casaccio, quindi è necessario valutare bene quali sono le finalità dei trattamenti e quali sono le basi giuridiche adeguate.

Non solo, ma **i consensi devono essere gestiti**. Sia le preferenze cookies, sia i consensi per l'invio di newsletter e marketing non devono essere click vuoti, che si disperdono nell'etere, ma essere adeguatamente **conservati nel back end del sito e monitorati costantemente**.

Inoltre, poiché dovrebbe essere ugualmente semplice prestare un consenso e ritirarlo, il footer del sito dovrebbe prevedere, in ogni pagina, un link per la gestione ed il ritiro dei consensi da parte dell'utente.

Diritto & Diritti ISSN 1127-8579

5.La scelta dei fornitori

Infine, come dicevano i nostri saggi nonni, chi più spende meno spende. Non è detto che il fornitore più economico si riveli il più conveniente, e non solo per una questione di competenza.

I fornitori del nostro sito devono, a loro volta, essere compliant al GDPR. Quindi dovremmo preoccuparci di sapere dove si trova il server su cui poggia il sito, quale sistema di email marketing automation viene utilizzato, quale piattaforma per la gestione dei pagamenti è più adeguata e ricordarci di nominare i fornitori responsabili esterni del trattamento, oppure valutare se si tratti di Titolari autonomi. I dati che transitano sul nostro sito, infatti, di cui siamo noi i Titolari, verranno visti anche da terzi, ed è fondamentale **definire e stabilire i ruoli in merito al trattamento,** ancora una volta per ottemperare al requisito più importante di tutti quando si tratta di data protection, ovvero l'accountability del Titolare.

>> GUARDA il VIDEO sulle 5 regole d'oro per avere un sito web a prova di GDPR <<

[embed]https://youtu.be/v2HAn3mye08[/embed]

Nuovo volume:

Diritto & Diritti ISSN 1127-8579

https://www.diritto.it/come-avere-un-sito-web-a-prova-di-gdpr-5-regole-doro/

Diritto & Diritti ISSN 1127-8579