GDPR WordPress per Aziende e professionisti

Guida Pratica

Guida all'applicazione del regolamento europeo in materia di protezione dei dati personali per proprietari di siti web professionali realizzati con Wordpress o Woocommerce

Loredana Ciardone
info@loredanaciardone.com

GDPR WordPress per Aziende e professionisti

Indice

Guida completa su:

https://www.sito-wp.it/guida-gdpr-siti-wordpress/

Capitolo 1 (GDPR WordPress)

Iniziare a capire il GDPR

Il regolamento generale sulla protezione dei dati (GDPR) è una nuova legge che è stata messa in lavorazione da alcuni anni ed'è stata finalmente approvata nel 2016. Dopo un periodo di transizione di due anni, entrerà finalmente in vigore dal 25 maggio 2018.

Questa legge sostituisce il suo precedente regolamento del 1995 con linee guida aggiornate che governano e proteggono la privacy delle persone nell'Unione europea.

Il GDPR è un regolamento, non una direttiva. E senza entrare nei dettagli ciò significa che non è solo un consiglio, è una legge. Questo è molto importante per l'Unione e devi fare attenzione a rispettarlo.

Ecco qui per i più poliglotti una bella infografica della Commissione Europea sul GDPR.

Qual è lo scopo del GDPR?

Lo scopo di questa nuova serie di regolamenti è piuttosto complesso ma principalmente focalizzato sul dare ai cittadini dell'UE più controllo sui propri dati personali, che condividono con i siti web (ma soprattutto con le aziende che stanno dietro questi siti web).

Questo cambierà quindi l'approccio diverso di aziende e organizzazioni di tutto il mondo verso la privacy, la gestione dei dati, la raccolta dei dati, la sicurezza e la profilazione dei loro utenti.

Riassumendo:

Il GDPR mette davvero in discussione l'idea che siano le persone – al contrario delle aziende – ad avere il diritto di proteggere i propri dati personali. Chiamandolo "diritto", l'UE chiarisce quanto sia importante e forte il suo desiderio che le imprese interpretino questa legge.

Quali sono i diritti per cui il GDPR entra in gioco?

I seguenti diritti individuali sono quelli evidenziati dal GDPR:

- Diritto di essere informato [Capitolo # 3; Art. 12]
- Diritto di accesso [Capitolo # 3; Art. 15]
- Diritto di rettifica [Capitolo # 3; Art. 16]
- Diritto alla cancellazione [Capitolo # 3; Art. 17]
- Diritto di limitare l'elaborazione [Capitolo # 3; Art. 18]
- Diritto alla portabilità dei dati [Capitolo # 3; Art. 20]
- Diritto di opporsi [Capitolo # 3; Art. 21]

Oltre a questi, il GDPR offre anche disposizioni per il processo decisionale individuale automatizzato e il profiling.

Quali sono le conseguenze del mancato rispetto del GDPR?

Le conseguenze che derivano dall'ignorare le direttive GDPR sono piuttosto gravi.

Se la tua azienda violasse tali leggi, la pena è una sanzione fino a € 20 milioni di euro o il 4% dell'intero fatturato aziendale.

Dati tali numeri in gioco, dubito che ti sentirai di rischiare.

Il mio sito Web WordPress / o Sito e-commerce WooCommerce deve essere compatibile con il GDPR?

Certo che sì.

Se il tuo sito Web WordPress o il sito e-commerce creato con WooCommerce o Magento o qualsiasi altra piattaforma ecommerce raccoglie dati personali di utenti provenienti dall'UE, è necessario ottenere una conformità al GDPR.

In altre parole, tutti i siti Web che raccolgono le informazioni personali di individui e cittadini all'interno dell'UE rientreranno nella giurisdizione del GDPR.

Ok ora immaginiamo già l'espressione sul tuo viso: ti stai chiedendo cosa siano i dati personali, giusto?
Un indirizzo email è considerato dato personale, per esempio?

Non vendo nulla tramite il mio sito WordPress! Devo rispettare anche io il GDPR?

L'obiettivo del GDPR non è il tipo di sito Web o negozio che stai gestendo. Il regolamento non se ne preoccupa affatto.

La cosa principale su cui GDPR ingerisce sono i dati e quindi può influire anche su un semplice modulo di contatto che sta su una delle tue pagine.

Quindi:

Se hai un sito Web WordPress e disponi di un modulo di commento, e le persone mettono il loro nome e indirizzo email nel modulo di commento, stai raccogliendo un dato personale.

E se il tuo sito web è raggiungibile dalle persone che vivono nell'Unione europea, stai raccogliendo dati personali da persone nell'Unione europea.

Quindi ogni Sito web WordPress è potenzialmente toccato da questo nuovo regolamento.

Capitolo 2(GDPR WordPress)

Profilazione utenti e Dati del cliente sotto GDPR

Il regolamento generale sulla protezione dei dati dovrebbe essere applicato dal 25 maggio 2018. Come titolari di aziende si deve affrettarsi a saperne di più sugli aspetti che copre e sulle implicazioni che porterà con sé, c'è ancora molto che si deve essere scoprire in termini di applicazioni esatte dei regolamenti.

Un'area critica, tuttavia, ha a che fare con il modo in cui raccogli gli indirizzi email e come poi li usi.

Questo è quindi strettamente connesso a tutti i tipi di moduli che hai sul sito web o sito e-commerce Woo-Commerce e quanto sai dei tuoi utenti.

Indirizzi email, moduli, profilazione dell'utente, carrelli abbandonati, pagine di checkout. Come devo modificarli per rispettare il GDPR? Anche questo lo vedremo fra poco

Cosa è considerato un dato personale?

Come li definisce il regolamento (capitolo 1, articolo 4, punto 1):

Per "dati personali" si intendono tutte le informazioni relative a un identificativo o identificabile persona fisica ("soggetto interessato"); una persona fisica identificabile è colui/lei che può essere identificato, direttamente o indirettamente, in particolare facendo riferimento a un identificatore comeun nome, un numero di identificazione, dati di posizione geografica, un identificatore online o uno o più fattori specifici per il fisico, fisiologico, genetico, mentale, economico, culturale o identità sociale di quella persona naturale.

Per un sito web o un gestore di negozio, queste parole possono essere riassunte più facilmente nella grafica che segue:

La cosa importante da capire qui è questa! Dal momento che il tuo sito web è accessibile da ovunque nel mondo, in qualche modo raccoglie dati da individui all'interno dell'Unione Europea, quindi rientra nella giurisdizione del GDPR.

Questo regolamento afferma che tutto deve essere reso più cristallino che mai.

La nuova legge è stata specificamente progettata per garantire la protezione dei dati dei consumatori e la privacy e, di conseguenza, fornisce loro una nuova serie di poteri autorevoli per controllare i modi in cui i loro dati possono essere raccolti e utilizzati dai siti Web.

A questo proposito, il GDPR cambia quella che era la normale routine di raccolta del maggior numero di dati possibili riguardo a un utente a fini di marketing.

In altre parole con il GDPR, cambierà il modo di profilare gli utenti.

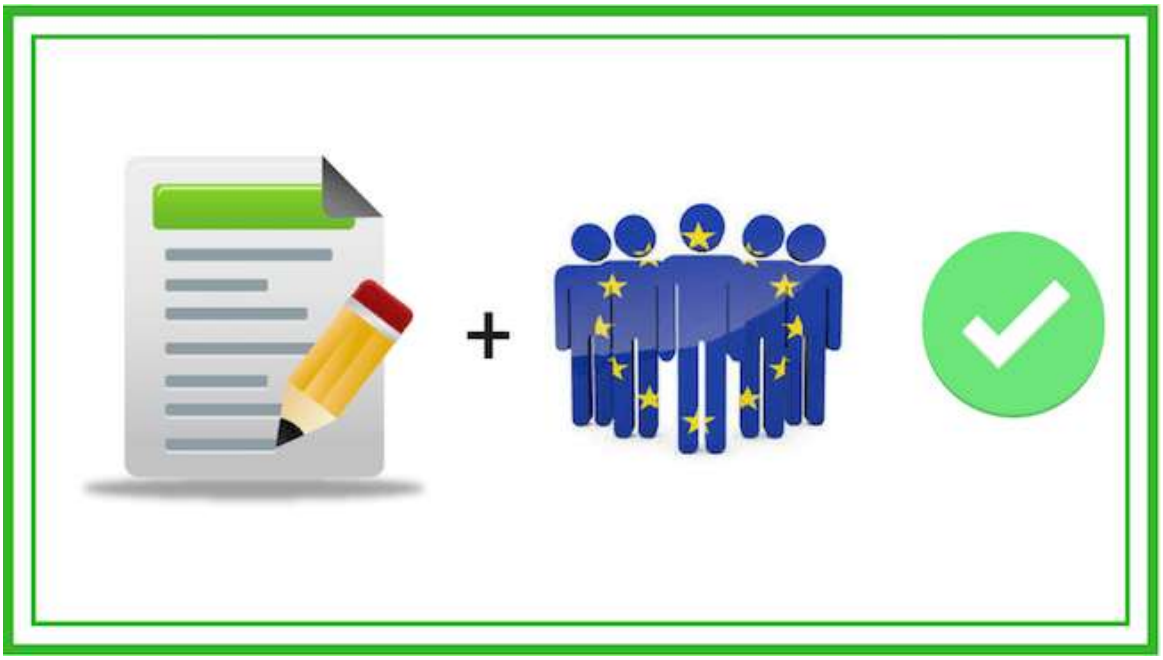
Regolamenti GDPR relativi alla profilazione per scopi di marketing

Iniziamo con la definizione di profilazione, che è discussa sotto la sezione "Diritti del data subject "capitolo 3, articolo 12, ma è meglio presentata nel Recital 71:

Che cos'è la profilazione con GDPR?

> *La profilazione consiste in qualsiasi forma di elaborazione automatizzata di dati personali valutando gli aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti le prestazioni dell'interessato sul posto di lavoro, situazione economica, salute, preferenze o interessi personali, affidabilità o comportamento, posizione o movimenti, ove produca effetti legali che lo riguardano o in modo simile colpiscano in modo significativo lui o lei.*

La profilazione è sempre stata vista come una procedura standard per i proprietari di siti Web e negozi, ma ora con il GDPR, gli utenti dovranno essere informati sul trattamento dei loro dati e come esercitare i loro diritti.



Moduli e raccolta dati dei clienti sotto GDPR

Una gran parte dei dati dell'utente viene raccolta attraverso i moduli di contatto proprio nella pagina contatti, pagine di checkout, moduli per richiedere informazioni o un preventivo, landing page per scaricare per scaricare una risorsa gratuita.

Di solito, è su questi moduli che chiediamo più di quello che dobbiamo effettivamente raccogliere. Un esempio comune è rappresentato da un campo nel nostro modulo che richiede un qualche tipo di informazione non strettamente pertinente in quel momento ma che riteniamo lo sarà in futuro.

Questo non è accettabile ai sensi del GDPR, quindi:

Se hai un elemento nel modulo di acquisizione dati o nella pagina di checkout di cui pensi 'Non ne ho bisogno ma potrei usarlo in futuro'. bene, se per quel futuro momento non avrai ottenuto il consenso, tecnicamente parlando, non dovresti quindi usarlo per la profilazione, in quel caso starai infrangendo il GDPR, quindi in pratica se lo vuoi, devi raccogliere quel dato fuori dal tuo modulo o ottenere il consenso ad usarlo per la profilazione.

Come chiedere indirizzi stradali

Gli indirizzi stradali sono un caso più specifico relativo all'e-Commerce o Siti web basati su Woo-Commerce che richiedono queste informazioni durante il checkout e sono trattati allo stessa stregua degli indirizzi e-mail sotto il GDPR.

Spieghiamo:
Puoi chiedere l'indirizzo alla fine per la convalida della carta di credito, a seconda del fornitore di servizi di pagamento che stai utilizzando.

Quindi la regola di cui sopra, continua a reggere: se la transazione non funziona senza l'indirizzo, allora è necessario raccogliere questo dato utente, quindi sicuramente puoi.

D'altra parte, se non ne hai strettamente bisogno per processare l'acquisto e il pagamento, valuta di non raccoglierlo. Gli indirizzi stradali sono importanti nei download digitali e nei pagamenti online perché il crimine informatico e le frodi sono uno dei maggiori fastidi del commercio elettronico oggi e se un cliente sta usando una carta rubata, questa può essere verificata analizzando se l'indirizzo fornito corrisponde a quello della carta.

E' importante ricordare che non è necessario il consenso per raccogliere dati personali che sono necessari per la transazione. Quindi, la richiesta di indirizzi stradali non è particolarmente problematica, perchè essenziale dato per perfezionare un ordine.

Il problema nasce invece con i carrelli abbandonati e le pagine di pagamento. Attenendosi alle questioni relative alla profilazione per il marketing, i carrelli abbandonati alla cassa sono una zona grigia, questo perché un alcuni negozi online catturano l'indirizzo e-mail del cliente non appena inserito, anche quando non completano il rispettivo acquisto.

Quindi:

Il problema con i carrelli abbandonati e il checkout abbandonato per gli utenti che non hanno acquistato da te è una grande area grigia.

E quando dico area grigia, voglio dire, che un'interpretazione del GDPR potrebbe indicare che le pratiche attualmente in uso per il carrello abbandonato costituiscono una violazione del ***requisito del consenso***. Molti negozi acquisiscono l'indirizzo e-mail prima di aver compiuto azioni e quindi inviano un messaggio e-mail un paio di giorni dopo dicendo:

"Abbiamo notato che hai riempito questo nel carrello. Vuoi riprendere ora il tuo acquisto? "

Come è stato raccolto il consenso lì?… Non è stato per caso raccolto?

La prima risposta a questa domanda cruciale è che:

non hanno ottenuto alcun consenso esplicito da parte del cliente.

Quindi, se stai semplicemente raccogliendo in silenzio gli indirizzi e-mail dalle tue pagine di pagamento e non fai nulla per ottenere un consenso esplicito, è molto probabile che ciò **non** rientri nello spirito del GDPR.

Quindi, come si può ottenere un consenso esplicito per inviare e-mail per riprendere un carrello abbandonato?

È difficile fornire una soluzione valida per tutti, senza conoscere il tuo caso specifico, ma ce n'è uno relativamente semplice da implementare.

In particolare, come per altri tipi di moduli, devi avere la possibilità di far dare esplicitamente il permesso – ***"spuntare per attivare"*** – per memorizzare i dati dell'utente attraverso il tuo modulo di verifica.

Ma non solo; in questo specifico scenario, il tuo modulo dovrebbe avere anche una sorta di spiegazione di quando inizia il processo di checkout, perché è da quel momento che è necessario il consenso esplicito per raccogliere i dati dell'utente.

Quindi:
Non puoi semplicemente dire sui tuoi moduli: ***"Accetto l'utilizzo dei dati su questo sito"*** perché questo non riguarderà i carrelli abbandonati ".

Dovresti avere, per esempio, qualcosa che dica: ***"la procedura di pagamento non inizia se nessuno è espressamente d'accordo alla raccolta di carrelli abbandonati"*** e mettere in atto una funzionalità personalizzata che si innesca se le condizioni sono soddisfatte.

Questo sarebbe un assenso. Ma, e questo è importante, è ancora necessario consentire di terminare il pagamento se l'utente non accetta la procedura del carrello abbandonato. Non puoi negargli il servizio basato su questo.

Non si deve mai dimenticare che, in base al GDPR, non è consentito abilitare un servizio se la gente ha rinunciato ad esso.

L'opt-in silenzioso o soft non è più accettabile per il consenso di GDPR.

Invio di e-mail ai tuoi clienti e utenti sotto GDPR

Moduli di contatto, pagine di checkout incomplete, pagine per download di risorse e simili, hanno tutti lo stesso scopo: raccogliere l'indirizzo email di qualcuno e ulteriori dettagli. Ecco perché dopo che il GDPR entrerà in gioco, le cose cambieranno. Uno dei principali problemi con le

informazioni personali raccolte sui siti Web è che, una volta create le liste email, alcuni bombardano la casella di posta del cliente con email promozionali. Oppure segmentano le loro mailing list e iniziano a promuovere un prodotto completamente diverso per le stesse persone (che non hanno optato).

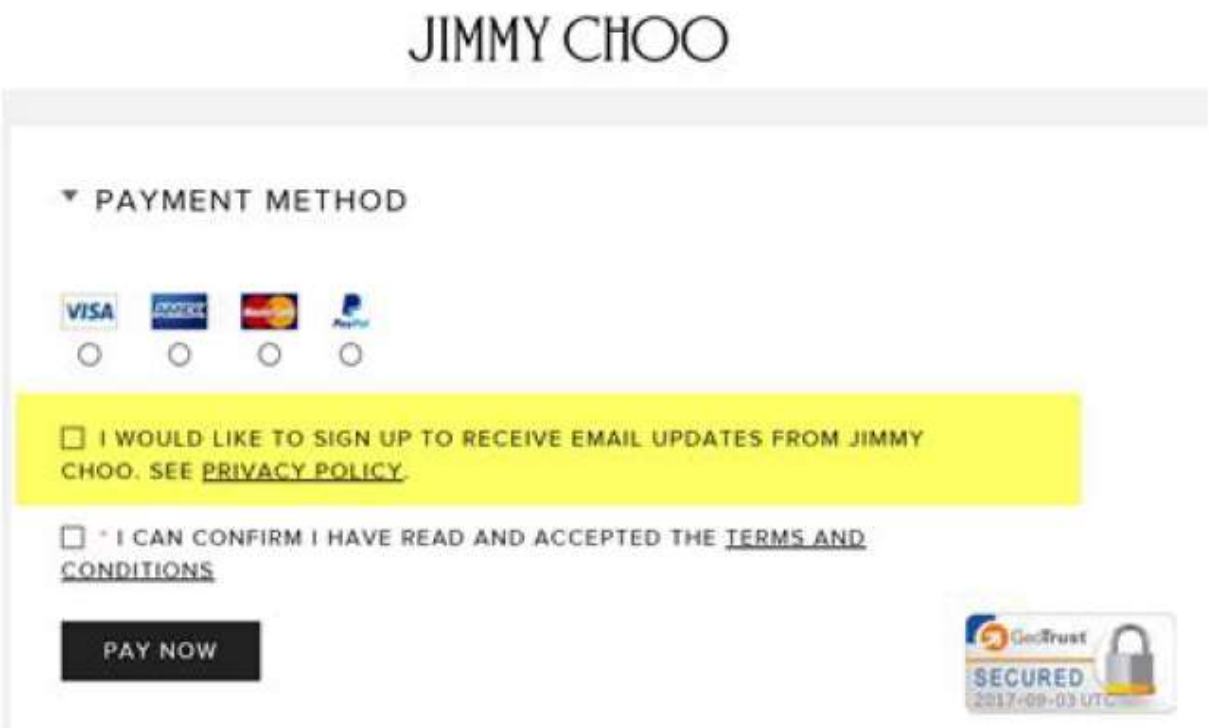
Ecco su cosa concentrarti: l'opt-in e per che cosa opta la gente.

Se la tua newsletter menziona sempre prodotti e invii link di affiliati – dovresti rivelarlo – sono il tuo lavoro! Va bene, perché i tuoi utenti hanno dato il consenso. Tuttavia, il GDPR ti colpirà molto se prendi questi clienti che hanno optato per la tua newsletter e li inserisci in un elenco separato per inviare pubblicità, che è un lavoro completamente diverso, e questo sarebbe una violazione della privacy del cliente.

Anche qui, l'opt-in silenzioso o soft non è più accettabile. Quindi, per esempio: Caselle per iscriversi alla newsletter pre-smarcate dovranno essere rimosse come recita il recital 32,:

Silenzio, caselle pre-spuntate o inattività non costituiscono assenso.

Come ottimo esempio, citiamo il negozio online di Jimmy Choo:



Capitolo 3 (GDPR WordPress)

Come preparare il tuo Sito Web WordPress o WooCommerce per il GDPR?

La risposta in breve, prepara una strategia. Una strategia che permetta di raccogliere, e archiviare dati e proteggerli come richiede il regolamento. ma anche una che preveda le procedure che ogni gestore di siti web / o negozio dovrà implementare in caso di violazione dei dati, portabilità dei dati, e la cancellazione dei dati. Questo è un buon punto di partenza infatti la cosa principale su cui punta il GDPR è l'arricchimento della sicurezza dei dati personali.

E questo passa attraverso una revisione della strategia di raccolta dei dati degli utenti, che va al di là di come li gestisci e memorizzi.

Nello specifico, devi modificare tutto il contenuto e deselezionare tutte le opzioni dei tuoi moduli. Quindi lascia che le persone si iscrivano senza dar loro qualcosa direttamente, che non è espressamente richiesto, chiedi quindi chiaramente il consenso del cliente.

Ottenere il consenso può rendersi difficile sui siti WordPress WooCommerce.

La caratteristica più basilare introdotta da GDPR è che, sebbene la richiesta di consenso fosse in atto già prima, ora deve essere chiesta in modo molto chiaro ed esplicito.

Quindi:

Il consenso deve essere chiaro, molto chiaro. La parola usata nel testo del regolamento GDPR è "inequivocabile".

Quindi non può esserci più un: "Accetto, che i miei dati potrebbero essere inseriti in una lista di newsletter".

No, deve dire **"Accetto, che i miei dati siano usati a fini di Marketing e inseriti in una lista newsletter Pubblicitaria"** e quindi devono esserci chiari riferimenti specifici, a come quei dati verranno utilizzati.

E così via in tutti gli altri punti di contatto del sito web o negozio online.

Inoltre, il consenso deve essere espresso per ciascuno degli scopi per cui si stanno raccogliendo dati e ancora si deve raccogliere il consenso in ogni occasione in cui il dato venga richiesto, anche se più volte in pagine diverse.

In fine devi descrivere il motivo per cui lo stai usando.

Per i form di WooCommerce sono necessarie delle modifiche per renderli conformi.

Premettiamo che è in fase di Testing la versione Woocommerce 3.4 che avrà delle novità in termini di GDPR.

Alcune caratteristiche sono:

- Possibilità di aggiungere testo della privacy policy alle pagine di checkout e account
- Strumenti per ripulire (trash) e rendere anonimi vecchi ordini che non richiedono più l'elaborazione.
- Strumenti per rimuovere alcuni campi opzionali dal checkout.

Quindi:
Nel contesto WooCommerce, ci sono un paio di complicazioni che potrebbero essere più complesse da gestire per ottenere il consenso su:

- carrelli abbandonati,
- ordini di pagamento abbandonati
- la segmentazione dei clienti basata sugli ordini.

(Per esempio se stai usando un servizio come MailChimp, e l'hai collegato ai dati del tuo sito e-Commerce che segmenta i clienti in base ai precedenti acquisti.)

Per cose come questa, avrai bisogno di ottenere il consenso, e questo diventa piuttosto complesso nell'area di check out, perché dovrai aggiungere un'area di consenso in più.

Come titolare di un sito e-commerce dovrai ragionare su alcune domande che saranno strettamente correlate alle decisioni aziendali, come:

- Ok, cosa è più importante per noi?
- In quale caso, avremo bisogno di ottenere un consenso specifico?
- Dovremo smettere di segmentare i nostri utenti come facciamo ora?

Quali sono le primissime cose che devono essere implementate per essere conformi al GDPR?

Ci sono un certo numero di funzionalità che devono essere implementate in conformità con questa nuova legge, 3 sono le aree principali. 3 aspetti su cui concentrarsi immediatamente per il sito web

- Notifica di violazione
- Raccolta, elaborazione e archiviazione dei dati
- In che modo i plug-in in esecuzione sul tuo sito web / negozio trattano i dati dall'utente

Per aiutarti, ci sono plugin gratuiti per WordPress già disponibili su repository.

1. **Discutere la situazione con i fornitori di servizi di terze parti**

Dato che il GDPR è interamente basato su dati e privacy, prima di tutto dovrai capire come tutti i fornitori di servizi che gestiscono i dati utente con cui lavori si approcciano al GDPR. Soprattutto, devi indagare su ciò che verrà fatto dato che il GDPR diventa effettivo a maggio.

Se hai un background tecnico e una buona conoscenza di GDPR, potresti fare una chiamata con i loro sviluppatori e richiedere informazioni nel merito dei loro rispettivi plugin / strumenti, a volte basta chiedere. Se non ti senti a tuo agio nel farlo, puoi chiedere a un esperto WordPress di verificare quali plugin stai usando e se questi abbiano bisogno di essere adeguarsi al GDPR.

Agli sviluppatori dei tuoi plugin potresti, qualcosa del tipo: "Pensiamo che il tuo strumento o il tuo servizio web possa infrangere il GDPR. Quali misure hai messo in atto per adeguarlo? Questi

potrebbero rispondere: “Ok qui, trovi la procedura di opt-in, è così appare sullo schermo poco prima del pagamento. Se le persone decidono di eseguire l’ opt-in, archiviamo i loro dati. Se dicono di no, lo spegniamo”. Questo è un aspetto importante di cui devi essere a conoscenza, in quanto un’azienda che utilizza uno strumento o servizio, deve comunicarlo nella proprio documento privacy. Ovviamente, tieni presente in quale misura strumenti o servizi di terze parti gestiscono i tuoi dati utente.

Fornitori di terze parti a cui vuoi chiedere in merito alla conformità GDPR:

- Hosting
- Provider di script di terze parti
- Spedizionieri e partner di spedizione
- Sviluppatori di plug-in che raccolgono e archiviano i dati utente attualmente utilizzati (o pianificati)
- I fornitori di servizi di invio email

2. Aggiorna la tua politica sulla privacy e le note sulla privacy

Considerato quanto sia vasto il dominio del GDPR per un sito Web o un negozio online, una revisione importante della tua attuale documentazione sui dati dell’utente e sulla privacy è decisamente necessaria.

Come richiesto nel Capitolo # 3, art. 12, è necessario trasmettere tutte le informazioni relative a come gestisci ed elabori i dati dell’utente con le seguenti modalità:

1. In un linguaggio chiaro e semplice;
2. Facilmente accessibile;
3. Conciso;
4. Trasparente;
5. Intellegibile;
6. Accesso al documento Gratuito;

Ciò significa, ovviamente, che la tua politica sulla privacy e le note sulla privacy potrebbero dover essere riviste per riflettere questi requisiti.

3. Aggiorna la tua politica sulla privacy e le note sulla privacy

Usa icone coerenti (e attendi fino a quando le icone standard saranno rilasciate)

Il consenso esplicito per ottenere informazioni personali è la chiave di volta del GDPR, ma non è l’unica base legale su cui appoggiarti. Qualsiasi sito web o negozio – anche il tuo – che raccoglie i dati personali e le informazioni dovrà esporre icone che faciliteranno i suoi utenti a capire nel dettaglio il consenso che stanno per dare.

Il GDPR è molto specifico a riguardo: le icone devono essere coerenti. E riguardo a questo, i legislatori che hanno creato il GDPR vogliono vedere uno standard globale, che è in arrivo per le icone relative ai dati personali.

Non c’è ancora nulla di pronto, ma molto presto lo sarà. Tenetevi pronti a vedere spuntare qualcosa a riguardo, molto a breve. Per un’idea migliore su queste icone sulla GDPR, ecco un progetto

accademico di Aza Raskin di Mozilla che ha sviluppato delle icone sulla privacy ispirate da Creative Commons che sembrano semplificare l'informativa sulla privacy.

Quindi:
I visitatori del tuo sito Web cominceranno ad abituarsi a vedere queste icone. Cominceranno a dire: "Ok, questa rappresenta il consenso su come sono utilizzati i miei dati. ' Oppure smarcheranno alla cieca il consenso perché sono già abituati all'icona.