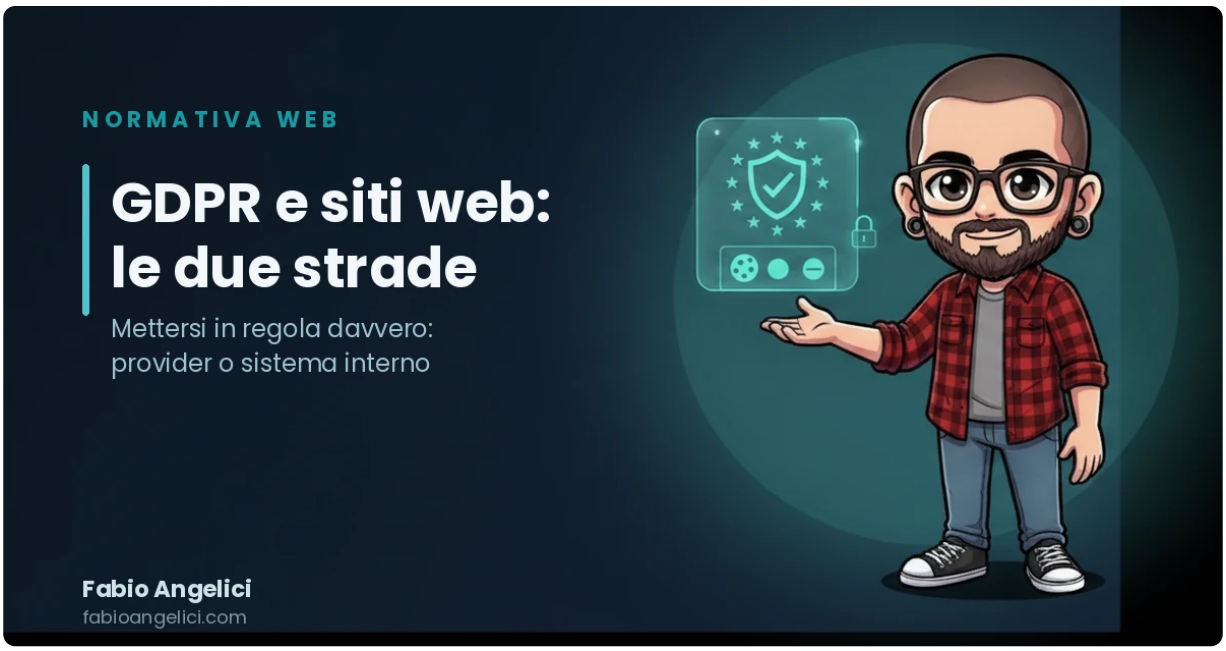
GDPR e siti web: le due strade per mettersi in regola

Di Fabio Angelici • Pubblicato il 28 luglio 2026 • 8 min di lettura

Gestione Aziendale | Normativa Web



RISPOSTA RAPIDA

Il GDPR non si esaurisce nel banner dei cookie. Cosa prevede la normativa per siti, e-commerce e applicazioni, e le due strade percorribili: appoggiarsi a un provider come iubenda o Cookiebot, oppure sviluppare il sistema in casa con i testi scritti da un avvocato. Con i criteri per scegliere.

Nota: Questo articolo è a scopo puramente informativo. Io scrivo codice, non pareri legali.
Per la tua situazione specifica serve un avvocato che si occupi di protezione dei dati:
qui trovi come funzionano le cose sul piano tecnico, non una consulenza.

Il GDPR è ormai in vigore da quasi 10 anni, tuttavia a volte quando vengo contattato
per un lavoro c'è sempre qualcuno che mi pone la domanda: "Ma è veramente necessario? e cosa rischio se non mi adeguo?"

Purtroppo il GDPR viene raccontato malissimo:
o come una scartoffia da spuntare e dimenticare, o come un mostro che ti multa di venti milioni per una casella sbagliata.
Non è né l'una né l'altra.

Cosa è il GDPR, senza giri di parole

È il Regolamento europeo 2016/679, applicabile dal 25 maggio 2018 in tutta l'Unione.
In Italia convive con il Codice in materia di protezione dei dati personali, rimasto in vigore in versione adattata.

L'idea di fondo sta in una riga: i dati personali delle persone non sono roba tua.
Te li affidano per uno scopo preciso, e tu li usi per quello scopo, per il tempo che serve, tenendoli al sicuro.

Dato personale è qualunque informazione che permetta di risalire a una persona, anche in modo indiretto.
Nome e email sono ovvi. Lo sono molto meno un indirizzo IP, l'identificativo di un cookie, l'ID di un dispositivo.

Chi decide perché e come trattare quei dati è il titolare del trattamento. Se il tuo sito raccoglie anche solo i contatti di un form, il titolare sei tu.
Non lo sviluppatore, non l'hosting: quelli semmai sono responsabili del trattamento, e vanno nominati per iscritto.

Un punto che sfugge quasi sempre: il consenso non è l'unica strada.
Le basi giuridiche previste sono sei, e per gestire l'ordine di un cliente basta l'esecuzione del contratto.
Chiedere il consenso per ogni cosa è un errore che si paga, perché il consenso si revoca in qualsiasi momento e a quel punto rimani senza appigli.

Sulle sanzioni si fa molta scena: il tetto arriva a 20 milioni di euro o al 4% del fatturato mondiale annuo.
Per una piccola impresa italiana il rischio concreto è un altro: il reclamo di un utente scocciato,
un'istruttoria del Garante e la corsa a rimettere tutto in ordine in due settimane.

Dove ti tocca davvero, su un sito

La normativa è scritta in astratto. Sul tuo sito diventa una manciata di punti concreti.

I form. L'informativa deve essere raggiungibile prima dell'invio, non nella pagina di ringraziamento.
E se il modulo serve a farsi ricontattare, il consenso a mandare offerte commerciali è un'altra cosa: va spuntato a parte, mai preselezionato.

I cookie e i tracciatori. Qui la regola arriva dall'articolo 122 del Codice, letto insieme alle Linee guida del Garante del giugno 2021,

pienamente applicabili dal 10 gennaio 2022. Sono i punti dove ho visto più siti scoperti:

- rifiutare deve essere facile quanto accettare, con un comando allo stesso livello
- la X che chiude il banner chiude e basta, non vale come consenso
- nessun cookie non tecnico parte prima della scelta dell'utente: il blocco è preventivo
- se l'utente ha detto no, il banner non si ripresenta a ogni visita, si aspettano almeno sei mesi
- deve esistere un punto sempre raggiungibile per cambiare idea

Un font caricato da un server esterno, una mappa incorporata o un video embeddato fanno partire una connessione verso terzi prima che l'utente abbia deciso alcunché. Non sono orpelli grafici, sono trattamenti.

L’e-commerce. Dati di ordine, pagamento e spedizione che passi a soggetti esterni: corriere, gateway, gestionale, email marketing.
Ogni passaggio va regolato con un contratto di nomina, e va deciso per quanto tempo conservi i dati.

Le applicazioni web. Log e backup: i primi tengono indirizzi IP, i secondi copie di dati che magari hai già cancellato.
Se un utente chiede la cancellazione, devi saper rispondere anche lì.

Prima strada: ti appoggi a un provider

È la scelta più diffusa, e per moltissime realtà è anche quella giusta.
Servizi come iubenda, Cookiebot e le altre CMP ti danno un banner pronto, privacy e cookie policy generate da un questionario, un registro dei consensi e la scansione periodica del sito.

I costi sono contenuti e prevedibili.
I piani di iubenda partono da poco meno di cinque euro al mese per sito, con fatturazione annuale e fino a 25.000 visualizzazioni di pagina,
salgono a una ventina di euro per il piano intermedio e a circa ottanta per quello superiore.
Il vantaggio vero non è il prezzo: è che quando la normativa cambia i documenti si aggiornano da soli.

Il rovescio: è un abbonamento, e se smetti di pagare i documenti restano lì senza più aggiornarsi.
I testi nascono da clausole standard e descrivono la tua attività per approssimazione.
Carichi uno script di terze parti su ogni pagina. E oltre una certa soglia di traffico il banner può spegnersi.

Seconda strada: te lo costruisci in casa

L’alternativa è sviluppare il sistema dentro il sito e far scrivere i testi a un legale.

Sul mio sito ho fatto così. Il banner è scritto da me e integrato nel codice, con blocco preventivo:
nessuno script non necessario parte prima che l’utente abbia scelto.
Le categorie sono quattro: cookie necessari, di statistica, di marketing e contenuti esterni.
La scelta finisce sul database, e una pagina dedicata permette di rivedere le preferenze quando si vuole.

I testi non li ho generati: me li ha scritti un avvocato specializzato in diritto digitale e protezione dei dati,
dopo aver guardato cosa fa davvero il sito. Il costo è stato di qualche centinaio di euro, una tantum.

Cosa ci guadagni: nessun canone a vita, nessuno script esterno, controllo su come e quando parte ogni tracciatore,
documenti che descrivono la tua attività e non una generica simile alla tua.

Cosa ci perdi: la manutenzione è un problema tuo.
Quando il quadro normativo si muove nessuno ti avvisa, devi accorgertene, chiamare il legale e aggiornare il codice.
Serve qualcuno che sappia mettere le mani nel sito, e quel qualcuno costa.

Quando conviene una e quando l’altra

La domanda dirimente non è quanto costa. È chi se ne occupa il giorno dopo.

Il provider ha senso se non hai nessuno che tocchi il codice, se gestisci più domini o più mercati,
se fai campagne pubblicitarie e ti servono le integrazioni pronte, o se vuoi togliere il pensiero e mettere una voce fissa a bilancio.

Il sistema interno ha senso se hai già un ufficio legale o un DPO, se il sito è seguito con continuità da qualcuno,
se hai esigenze che le clausole standard non coprono.

Esiste anche la via di mezzo, quella che consiglio più spesso alle aziende strutturate: testi scritti dal legale, banner e consenso affidati a una CMP.

Cosa bolle in pentola

A novembre 2025 la Commissione europea ha presentato la proposta nota come Digital Omnibus,
che punta a semplificare il consenso: regole sui cookie spostate dentro il GDPR, più casi in cui il consenso non serve,
accettazione e rifiuto con un solo clic, preferenze esprimibili dal browser.

Non è legge. È una proposta in mezzo alla procedura legislativa ordinaria.
Tienila d'occhio se stai per investire su un sistema nuovo, senza usarla come scusa per rimandare: oggi valgono le regole di oggi.

Cosa cambia in pratica

Il test più onesto lo fai da solo in due minuti. Apri il tuo sito in una finestra di navigazione anonima,
apri il pannello di rete del browser e guarda quali domini esterni vengono contattati prima che tu abbia cliccato qualsiasi cosa sul banner.

Se compaiono servizi di analisi, di pubblicità o di font, il banner sta facendo solo scena.
E se ne vedi partire di sconosciuti, hai già la risposta su dove sei messo.

Domande frequenti

Ho un sito vetrina senza form e senza analytics. Devo fare qualcosa?
Se non raccogli nulla e non carichi nulla da terze parti, gli obblighi si riducono parecchio.
Il punto è verificarlo, perché molti temi caricano font o mappe esterne senza dirtelo.

La privacy policy copiata da un altro sito va bene?
No, e il motivo è pratico prima ancora che legale: descrive trattamenti che non fai e ne omette altri che fai.
Un documento sbagliato è peggio di uno assente, perché dimostra che non hai guardato.

Google Analytics si può usare?
Sì, con consenso preventivo e una configurazione fatta bene.
La questione dei trasferimenti fuori dall'Unione resta delicata: se lo usi in modo intensivo, fattelo guardare da un legale.

Il mio hosting è conforme, lo sono anche io?
Sono due piani diversi. L'hosting è un fornitore e va nominato responsabile del trattamento, la conformità del sito resta in capo a te.

Il passo successivo

Se preferisci che quel controllo lo faccia io, e che ti dica quale delle due strade ha senso nella tua situazione e quanto costa percorrerla,
scrivimi e guardiamo insieme il tuo sito.

E se questa scelta l'hai già affrontata, sono curioso di sapere come è andata: provider o sistema interno? Scrivilo nei commenti.

FONTI

1. Regolamento (UE) 2016/679 (GDPR), testo consolidato
2. Garante per la protezione dei dati personali, Linee guida cookie e altri strumenti di tracciamento, 10 giugno 2021
3. Garante per la protezione dei dati personali, provvedimento del 27 febbraio 2025 su banner cookie non conformi
4. Commissione europea, proposta di regolamento Digital Omnibus (novembre 2025), analisi
5. Iubenda, pagina prezzi ufficiale
