

GDPR Cosa cambia per gli hotel e le strutture ricettive

https://site.edgarsmartconciierge.com/gdpr-cosa-cambia/#GDPR_cose

GDPR cos'è?

Il GDPR è il regolamento europeo su privacy e trattamento dati personali. GDPR significa General Data Protection Regulation, di cui è l'acronimo. Il **GDPR è il regolamento europeo sulla privacy** e stabilisce in che modo gli enti pubblici e le attività commerciali, compresi hotel e strutture ricettive, devono utilizzare:

- i dati sensibili delle persone (nome, cognome, indirizzo, ecc.)
- gli indirizzi IP
- i cookie

Perché abbiamo pubblicato proprio ora questa news su un argomento così impegnativo, soprattutto per chi non ama il linguaggio giuridico? Perché il GDPR, esattamente il Regolamento UE 679/2016 (puoi scaricare qua il [pdf in italiano del GDPR](#)), entrerà in vigore il 25 maggio 2018. Entro questa data la tua attività dovrà essere in regola con le nuove norme. Con una complicazione: il regolamento riguarda anche i dati raccolti ed elaborati prima di maggio 2018.

GDPR cosa cambia

Fino ad oggi la tutela della privacy e il trattamento dei dati degli italiani erano regolamentati dal D.lgs 196/2003. Dal 25 maggio 2018 il regolamento europeo sulla privacy prevarrà sul codice italiano in materia di protezione dei dati personali. Come sempre accade in ambito giuridico, sicuramente il legislatore italiano e gli organi competenti dovranno intervenire nei prossimi mesi per fornire dei chiarimenti. Dubbi e incompatibilità sono inevitabili nel passaggio da una legge italiana a una europea.

Novità e principi del GDPR 2018

Vediamo le **novità più importanti del regolamento europeo sulla privacy**, senza entrare nel dettaglio dei tecnicismi giuridici. Se può consolarti: non cambierà proprio tutto. Alcune norme sono invariate, altre sono state modificate. Ma ci sono anche delle novità assolute e quindi degli obblighi che non puoi ignorare per evitare le sanzioni.

Diritto all'oblio

La persona interessata avrà il diritto di chiedere all'attività commerciale la cancellazione dei dati personali. L'attività dovrà eliminarli se esiste almeno uno dei seguenti motivi, come si legge nell'art. 17:

- “i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso e se non sussiste altro fondamento giuridico per il trattamento;

- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- i dati personali sono stati trattati illecitamente;
- le informazioni personali devono essere cancellate per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.”

Data controller e data processor

Il GDPR 2018 introduce due figure, **Data Controller** e **Data Processor**, che in realtà esistono già nel Codice della Privacy italiano:

- il Data Controller è il titolare del trattamento dei dati, ovvero qualunque organizzazione in possesso dei dati personali dei cittadini europei;
- il Data Processor è il responsabile del trattamento dei dati, ovvero l'organizzazione che tratta i dati per conto del titolare.

A questi bisogna aggiungere il DPO, **data protection officer**, il responsabile della protezione dei dati.

La notifica della violazione dei dati

Il regolamento europeo stabilisce che in caso di violazione nella procedura di sicurezza che comporti un pericolo per la libertà o i diritti dei cittadini, **il titolare del trattamento ha 72 ore per avvisare l'Autorità di Controllo.**

Il registro dei trattamenti

Il registro non è sempre obbligatorio, ma è preferibile adottarlo. Al suo interno devono essere descritti i trattamenti effettuati e le procedure di sicurezza messe in atto.

I principi del GDPR privacy

Il regolamento europeo sulla privacy si basa su alcuni principi. Conoscerne i principali, può aiutarti a capire meglio come gestire i dati dei tuoi clienti.

Responsabilizzazione. La nuova norma europea responsabilizza le attività in materia di trattamento dei dati. Abbiamo appena visto che il GDPR introduce due figure. Entrambe devono seguire le norme e sono soggette a sanzioni. Pertanto non puoi scaricare la responsabilità sul titolare del tuo booking engine.

Extraterritorialità. Il GDPR protegge la privacy dei cittadini europei e vincola qualsiasi attività che tratta o gestisce queste informazioni. Spostare i dati fuori dall'UE non è quindi una soluzione.

Protezione dei dati fin dalla progettazione. Con le nuove norme sulla privacy, vale il principio per cui non devi correggere ma prevenire. Ovvero organizzare il trattamento dei dati in modo che non ci siano violazioni prima che queste si verifichino. Il processo di gestione deve essere sicuro dall'inizio alla fine. In termini tecnici si dice **privacy by design**.

Privacy by default. La privacy e l'utente sono al centro del regolamento. I dati vanno trattati solo secondo modi e tempi sufficienti al raggiungimento dello scopo dell'attività che li raccoglie.

Regolamento europeo privacy: le sanzioni

Le sanzioni previste nel regolamento europeo privacy

Le nuove norme sulla privacy introducono delle **sanzioni amministrative** più salate. Le multe possono arrivare a 20 milioni di euro o al 4% del fatturato annuo globale. Tuttavia, gli addetti ai lavori pensano sia quasi impossibile che una piccola struttura ricettiva sia costretta a pagare cifre simili. Non pensare che per questo non sia necessario adeguarti al nuovo regolamento. Potresti rovinare l'immagine del tuo hotel e avere una perdita di clienti altrettanto costosa in termini di ricavi. Se vuoi approfondire, leggi questo articolo sulle [sanzioni previste dal GDPR 2018](#).

GDPR: cosa fare se gestisci un hotel o una struttura ricettiva

4 cose da fare se gestisci un hotel o una struttura ricettiva

Cosa cambia per un hotel o un qualsiasi tipo di struttura ricettiva con il GDPR 2018? Ecco 4 cose da fare subito per adeguarti al nuovo regolamento ed evitare sanzioni. Gli interventi da adottare cambiano a seconda del tipo e della quantità di dati che raccogli. Per farti un esempio: non tutte le strutture ricettive hanno un sistema di videosorveglianza. Più informazioni e tecnologie utilizzi, più sarà complessa la loro gestione.

1. Dai al cliente il modo di esprimere il suo consenso

Ogni cliente che ti invia i dati personali deve avere la possibilità di darti il consenso esplicitamente, deve capire come verranno usati i suoi dati ed essere attivo nel darti il consenso. Ad esempio, nel caso del form di iscrizione alla newsletter della tua struttura ricettiva deve poter spuntare la casella appositamente, non trovarla già selezionata. **È una tua responsabilità utilizzare un linguaggio chiaro e comprensibile a tutti.**

2. Richiedi l'autorizzazione all'uso dei cookie

Informa l'utente che utilizzi **cookie che raccolgono dati non in forma anonima ma personale** (come le e-mail, i numeri di telefono, etc.) Probabilmente sul tuo sito già compare la barra sui cookie. In caso contrario, inseriscila.

3. Scrivi un'informativa dettagliata sulla privacy

Sul tuo sito deve essere presente un'informativa dettagliata sulla privacy. Spiega bene nel documento quali dati raccogli, perché e come. Includi tutte queste informazioni: quelle che l'utente invia spontaneamente, quelle memorizzate dai cookie e quelle raccolte da altre tecnologie utilizzate. **Devi indicare il periodo di conservazione dei dati** e i criteri in base ai quali hai stabilito questo periodo di tempo.

Scarica gratis il [modello privacy per strutture ricettive](#) che abbiamo preparato per te.

4. Identifica il data controller e il data processor

Per ogni dato raccolto deve essere chiaro chi è il data controller e il data processor. Per quanto riguarda il **DPO (Data Protection Officer) non deve**

essere necessariamente interno (come per enti pubblici, attività che trattano dati giudiziari o operano su larga scala). Nel caso degli hotel e delle strutture ricettive, può essere un professionista esterno, un'associazione, un ufficio. Il DPO deve avere competenze informatiche, sulla sicurezza e la normativa europea per la protezione dei dati. Inoltre deve conoscere il settore e il modo in cui opera il titolare del trattamento.

Infine, un suggerimento. Se gestisci una piccola struttura ricettiva, questi 4 semplici accorgimenti dovrebbero bastare a proteggerti da eventuali sanzioni. Ma se hai un hotel o sei un property manager con decine di case vacanza, richiedi una consulenza a un professionista specializzato in privacy.