HotellerieSuisse

Il nuovo Regolamento generale UE sulla protezione dei dati (GDPR) – Applicabilità e implicazioni per il ramo alberghiero svizzero (Ultimo aggiornamento: dicembre 2017)

1. Applicabilità del GDPR per le imprese svizzere

Il nuovo Regolamento generale UE sulla protezione dei dati (GDPR) è entrato in vigore il 25 maggio 2018. La sua validità tocca sia le imprese con sede nell'UE, sia alcune aziende svizzere come quelle che offrono merci e prodotti a clienti dell'UE e che ne trattano i dati personali (nome, indirizzo postale ed e-mail, data di nascita, coordinate bancarie, ecc.) ai fini della transazione.

Gli hotel svizzeri sono quindi tenuti a rispettare il nuovo GDPR quando vendono i loro servizi (alberghieri) ai cittadini UE all'interno dell'UE. Ciò riguarda soprattutto i siti web attraverso i quali tali clienti fanno le loro prenotazioni. Il Regolamento non riguarda invece le aziende che offrono servizi solo al mercato svizzero.

Premesso tutto ciò, si può dare per scontato che la maggior parte degli alberghi sia soggetta al GDPR nella misura in cui trattino i dati personali dei cittadini UE.

Per «trattamento» si intende la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione di dati personali.

2. I principi fondamentali del GDPR

- **Liceità, correttezza e trasparenza**
  I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

- **Limitazione della finalità**
  Il trattamento deve perseguire finalità esplicite e i dati vanno trattati solo in modo compatibile con tali finalità.

- **Minimizzazione dei dati**
  Possono essere trattati solo i dati necessari al raggiungimento delle finalità (per cui sono trattati).

- **Correttezza**
  I dati personali devono essere esatti. Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti.

- **Limitazione della conservazione**
  I periodi di conservazione dei dati personali vanno limitati al minimo necessario.

- **Integrità e riservatezza**
  Il trattamento deve garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

- **Responsabilizzazione**
  Il titolare del trattamento risponde del rispetto dei principi descritti e deve poter dimostrarne l'osservanza. In conformità al GDPR, il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o

altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

3. Le disposizioni principali del GDPR (elenco non esaustivo)

3.1 Liceità del trattamento

Il trattamento (ad esempio la prima raccolta di dati degli ospiti) è lecito solo se e nella misura in cui ricorra almeno una delle seguenti condizioni:

- Il trattamento è necessario all'**esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso (ad esempio alla stipula di un contratto d'albergo o alla prenotazione).

- I trattamento è necessario **per adempiere un obbligo legale** al quale è soggetto il titolare del trattamento (ad esempio quello di far compilare agli ospiti una scheda di registrazione in albergo).

- Il trattamento è necessario per il **perseguimento del legittimo interesse del titolare del trattamento o di terzi** (ad esempio la pubblicità diretta agli ex ospiti), a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

- L'interessato deve aver espresso il **consenso** al trattamento dei suoi dati personali.

Il **consenso** dovrebbe essere espresso mediante un atto positivo inequivocabile (ad es. vistando una casella di spunta). Il consenso tacito o dato cliccando su una casella di spunta già vistata o da vistare attivamente (cosiddetto opt-out) non soddisfano questi requisiti.

Per il trattamento di **dati sensibili** come quelli biometrici (ad esempio foto e impronte digitali) o riguardanti la religione e lo stato di salute è sempre necessario il consenso espresso dell'interessato.

Qualora siano previsti diversi trattamenti dei dati, l'interessato deve dare il suo consenso a ogni singola attività di trattamento.

L'interessato può revocare il suo consenso in qualsiasi momento. Il consenso deve poter essere revocato con la stessa facilità con cui è stato accordato (ad esempio cliccando sul link «Disiscriversi» in calce alle newsletter).

Attenzione: è obbligatorio comunicare all'interessato che può revocare il suo consenso prima che lo dia.

Se i dati vengono trattati per finalità di marketing diretto, l'interessato deve poter opporsi a questo trattamento in qualsiasi momento e gratuitamente. È necessario informare espressamente l'interessato che ha questo diritto. Ciò deve essere comunicato in modo comprensibile e distinto rispetto ad altre informazioni.

Esempi di formule:

"La parte contrattuale acconsente alla registrazione dei suoi dati personali (ad esempio nome e indirizzo e-mail) a cura dell'Hotel XX per … (ad es. l'invio di newsletter o mail per la pubblicizzazione dei servizi dell'albergo). Il consenso può essere revocato in qualsiasi momento presso ... (dati di contatto, indirizzo e-mail)."

3.2 Diritti dell'interessato e obblighi del responsabile del trattamento

- **Obblighi d'informazione**

È obbligatorio comunicare all'interessato che l'azienda tratta dati personali. Ciò vale anche nel caso in cui non vengano raccolti direttamente presso l'interessato stesso. Tale informazione deve essere comunicata in forma precisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni vanno fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

In caso di prenotazione eseguita, ad esempio, tramite il sito web dell'hotel le informazioni devono essere direttamente reperibili. Tutt'al più, possono essere segnalate inserendo un link al relativo documento/sito web nella conferma di prenotazione.

Le informazioni devono comprendere imperativamente quanto segue:

- l'identità e i dati di contatto del titolare del trattamento
- i dati di contatto del responsabile della protezione dei dati, ove applicabile
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento
- i legittimi interessi perseguiti (nella misura in cui siano stati indicati come motivo del trattamento)
- i destinatari o le eventuali categorie di destinatari
- ove applicabile, l'intenzione del titolare del trattamento di trasferire i dati personali a un paese terzo o a un'organizzazione internazionale
- il periodo di conservazione dei dati personali
- l'esistenza del diritto dell'interessato di chiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati
- l'esistenza del diritto di revocare il consenso in qualsiasi momento
- il diritto di proporre reclamo a un'autorità di controllo
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati
- eventualmente: l'esistenza di un processo decisionale automatizzato, compresa la profilazione (ad es. la verifica automatizzata della solvibilità)
- qualora i dati non siano stati ottenuti presso l'interessato: la fonte dei dati, specificando eventualmente se si tratta di una fonte accessibile al pubblico
- informazione sull'eventuale modifica della finalità del trattamento.

- **Diritto di accedere ai dati**

L'interessato ha il diritto di sapere se e quali dati personali vengono trattati dall'azienda, di essere informato sulle finalità del trattamento, sulle categorie dei dati rilevati, sui destinatari (o categorie dei destinatari), sui periodi di conservazione, sul diritto dell'interessato di chiedere la rettifica, cancellazione e limitazione dei dati, sul diritto di opporsi, di presentare reclamo, di conoscere la provenienza dei dati e, se del caso, l'eventuale esistenza di un processo automatizzato di decisione.

- **Diritto alla rettifica e alla cancellazione**

L'interessato ha il diritto di ottenere la rettifica dei dati personali che lo riguardano. I dati vanno cancellati immediatamente quando, ad esempio:

- non sono più necessari allo scopo per cui erano stati raccolti

- l’interessato abbia revocato il suo consenso e non sussistano altre basi giuridiche per la conservazione dei dati (ad es. obblighi legali)
- l’interessato si sia opposto al trattamento.

- **Diritto alla portabilità dei dati**

L'interessato ha il diritto di ricevere dal titolare del trattamento (ad es. l’albergo) i dati che lo riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico. L’esercizio di questo diritto presuppone che il trattamento iniziale si fondi su un consenso o un contratto e sia effettuato con procedimenti automatizzati.

- **Diritto di opposizione**

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati. Se si oppone, ad esempio, al trattamento finalizzato all’invio di pubblicità diretta, i suoi dati non possono essere più trattati per quella finalità.

3.3 Altri doveri del responsabile del trattamento (elenco non esaustivo)

- **Obbligo di eseguire una valutazione d’impatto sulla protezione dei dati**

La valutazione d’impatto sulla protezione dei dati è un’analisi dei rischi da effettuare prima del trattamento dei dati personali. La valutazione deve comprendere una descrizione sistematica dei trattamenti previsti, i rischi per l’interessato e le misure con cui limitarli o ridurli. La valutazione d’impatto riguarda però solo i trattamenti dei dati ad alto rischio (ad es. dati sanitari trattati dalle casse malati) per i diritti e la libertà degli interessati (ad es. clienti, utenti, collaboratori, ecc.). Nel caso standard, gli hotel non dovrebbero trattare dati di questo tipo.

- **Protezione dei dati fin dalla progettazione e per impostazione predefinita**

Il titolare del trattamento deve mettere in atto delle misure che rispondano al principio della protezione fin dalla progettazione (data protection by design) e per impostazione predefinita (data protection by default). Il titolare del trattamento deve quindi garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

- **Obblighi di documentazione**

I responsabili del trattamento devono tenere un registro (scritto o elettronico) delle attività di trattamento effettuate che contenga, tra le varie indicazioni, i seguenti punti:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento
- una descrizione delle categorie di interessati e delle categorie di dati personali (ad es. clienti e fornitori, dati per la fatturazione, indirizzi)
- le categorie di destinatari cui i dati personali sono stati o saranno comunicati (ad es. polizia e assicurazioni sociali), compresi i destinatari di paesi terzi od organizzazioni internazionali (società madre negli USA)
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate per proteggere i dati.

4. Sanzioni pesanti in caso di violazione degli obblighi

L'UE minaccia sanzioni pesanti. In caso di violazioni minori come quella degli obblighi dei responsabili del trattamento, si rischia di pagare fino a 10 milioni di Euro o il 2% del fatturato mondiale dell'anno precedente. In caso di grave violazione, le sanzioni possono arrivare a 20 milioni di Euro o al 4% del fatturato mondiale dell'anno precedente.

5. La Protezione dei dati in Svizzera

La Svizzera sta rivedendo la sua Legge sulla protezione dei dati. Il testo comprenderà molte disposizioni del GDPR, che verranno recepite con poche o senza modifiche. Il nuovo avamprogetto deve ora passare per la consultazione parlamentare. La revisione della LPD dovrebbe entrare in vigore all'inizio del 2022. Anche per questo raccomandiamo di familiarizzare sin da ora con l'argomento.

6. Come procedere

- Stabilisca chi sia/debba essere incaricato della protezione dei dati nella sua azienda.
- Verifichi quali dati personali vengono trattati dalla sua azienda (ospiti, collaboratori, fornitori, utenti del sito, ecc.), soprattutto quelli dei cittadini residenti nell'UE.
- Elabora dati sensibili (ad es. quelli relativi alla confessione e allo stato di salute)?
- Verifichi la base giuridica del trattamento (ad es. obbligo di legge, contratto, interesse legittimo, consenso).
- Verifichi se i dati siano effettivamente necessari. Se non lo sono, li cancelli.
- Verifichi la conformità dei suoi contratti, CGC e dichiarazioni sulla protezione dei dati al GDPR.
- Verifichi i processi/produca i documenti con cui adempiere ai suoi obblighi di informazione, documentazione, portabilità dei dati, ecc.
- Verifichi lo stato della sicurezza tecnica dei dati.

Altri ausili:

- HOTREC guidelines on the General Data Protection Regulation
- Check-list utili da scaricare dal sito della Wirtschaftskammer Österreich

Nota importante:

Questo foglio informativo presenta solo dei cenni sulle disposizioni UE sulla protezione dei dati. Il documento comprende l'essenziale e va quindi considerato uno strumento di orientamento non vincolante. Pur essendo state redatte con la massima solerzia, queste informazioni non hanno alcuna pretesa di completezza, correttezza e/o attualità.