



Libro bianco

Protezione dei dati e l'industria alberghiera

Zurigo 20 luglio 2018

hotelleriesuisse

www.hotelleriesuisse.ch

Monbijoustrasse 130 | casella postale | 3007 Berna

Meyerlustenberger Lachenal S.p.A

Avvocati – Attorneys at Law

www.mll-legal.com | www.mll-news.com

Zurigo | Ginevra | Zugo | Losanna | Bruxelles

Libro bianco sulla protezione dei dati e l'industria alberghiera

Il diritto sulla protezione dei dati in Europa ha subito un profondo cambiamento. A livello di Unione Europea, il 25 maggio 2018 è entrato in vigore il Regolamento Generale sulla Protezione dei Dati (RGPD). Stante tale presupposto, anche in Svizzera è in corso una revisione totale della legge sulla protezione dei dati. Al momento non è ancora stato stabilito quali modifiche concrete porterà con sé tale revisione, né quando tali modifiche verranno applicate.

Rimane stabilito, tuttavia, che il legislatore svizzero prenderà come riferimento in gran parte il modello

europeo. Le novità riguarderanno tutte le imprese ed organizzazioni dei diversi settori, nonché pressoché tutti i processi operativi. Anche l'industria alberghiera si trova pertanto di fronte ad una grande sfida.

In questo scenario, il presente libro bianco mette in evidenza, in un primo passaggio, il motivo per cui già l'entrata in vigore del RGPD è rilevante per le imprese e le organizzazioni dell'industria alberghiera svizzera. In un secondo passaggio, vengono spiegati i temi e le regole centrali, nonché gli interventi necessari che derivano da tutto ciò.

Indice

I.	La protezione dei dati interessa pressoché tutti i processi operativi!	4
II.	Perché il RGPD è rilevante per le imprese svizzere?	4
1.	Drastico inasprimento delle sanzioni in caso di violazione delle regole sulla protezione dei dati	4
2.	Quando sarà applicabile alle imprese svizzere il RGPD?	5
a.	Hotel svizzeri con succursale nell'UE	5
b.	Hotel svizzeri senza succursale nell'UE	6
III.	Cosa è necessario fare, ora, nel trattamento dei dati personali ovvero dei dati degli ospiti?	8
1.	In linea di principio, il trattamento dei dati personali è vietato, a meno che	8
2.	Principi fondamentali di ogni legittima elaborazione dei dati	9
3.	Nuova ed ampia "diligenza dovuta" nella gestione dei dati	9
4.	Quali diritti hanno le persone i cui dati vengono elaborati ("Diritti dell'interessato")	10
IV.	Direttive centrali per l'industria alberghiera	10
1.	Trasparenza dell'elaborazione dei dati	10
a.	Se i dati vengono raccolti direttamente dai vostri ospiti / partner commerciali	10
b.	Se i dati vengono acquisiti da fonti terze	11
2.	Consenso	12
a.	Volontà libera e divieto di collegamento	12
b.	Caselle preselezionate	12
3.	Passaggio di dati	13
a.	Informazioni generali	13
b.	"Parti terze"	13
c.	Trattamento dei dati su commissione	13
d.	Trasmissione all'estero	14
4.	Sistemi CRM	15
a.	Trasparenza e legittimità	15
b.	Finalità vincolata e modifica delle finalità	15
c.	Diritti di accesso e trasmissione	16
5.	Marketing per e-mail	16
a.	Consenso ("opt-in")	17
b.	Passaggio di dati a terzi e trasmissione all'estero	17
6.	Analisi del web / tracking	18
7.	Monitoring dei social media	19
8.	Giochi a premi	20
9.	WLAN dell'hotel	20

I. La protezione dei dati interessa pressoché tutti i processi operativi!

Le esperienze fatte sul campo mettono in evidenza che le imprese non sono affatto consapevoli di quanto incidano sulla loro quotidianità le regole della legge sulla protezione dei dati.

La legge sulla protezione dei dati viene applicata ogni volta che vengono trattati dati personali.

La portata della legge si evidenzia già dall'elencazione dei "trattamenti" rilevanti. Secondo la descrizione di legge, vi rientrano in particolare: "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".

❶ Esempio:

La legge sulla protezione dei dati non dovrà dunque essere osservata solo quando i dati di contatto di un ospite dell'hotel vengono comunicati ad un ufficio turistico, bensì anche **nelle operazioni puramente interne**, come quando l'ospite viene assegnato ad un segmento specifico di clienti nella banca dati.

Anche il requisito secondo cui deve trattarsi di "informazioni personali" non conduce ad una restrizione così ampia come spesso si presume. È certamente necessario che un'informazione possa essere associata a una determinata persona (fisica). Tuttavia, anche i dati resi come pseudonimi vengono considerati dati personali. Se dunque, ad esempio, in una banca dati i dati personali (nome, indirizzo, ecc.) di un ospite vengono sostituiti da un numero, i dati dell'ordine riferiti a questo numero sono ancora personali, se una persona all'interno dell'azienda o eventualmente addirittura

una terza parte sia in grado di assegnare nuovamente il numero all'ospite. La protezione dei dati viene quindi spesso trascurata nella gestione dei siti web.

❶ Esempio:

Se un utente cerca delle informazioni sul sito di Hotelleriesuisse per il suo prossimo soggiorno in Svizzera, semplicemente richiamando la home page lascerà una varietà di dati tecnici (specialmente l'indirizzo IP). Questi vengono (automaticamente) memorizzati sul server del sito web e devono essere trattati come dati personali per via della giurisprudenza in materia, anche se l'utente non ha o non ha ancora comunicato il proprio nome.

II. Perché il RGPD è rilevante per le imprese svizzere?

Due delle fondamentali innovazioni rispetto alla situazione giuridica precedente il mese di maggio 2018 spiegano la rilevanza del Regolamento Generale sulla Protezione dei Dati (RGPD) per le imprese svizzere. Da una parte, in caso di violazione delle regole incombono multe per importi milionari. Dall'altra, le regole del RGPD richiedono un'applicazione ben oltre i confini del mercato interno dell'UE.

1. Drastico inasprimento delle sanzioni in caso di violazione delle regole sulla protezione dei dati

Da parte dei sostenitori della privacy, la situazione giuridica prima dell'entrata in vigore del RGPD è stata criticata perché le sanzioni per le violazioni della protezione dei dati non erano sufficientemente deterrenti. Di conseguenza, anche le aziende dell'industria alberghiera, tra le altre, erano poco incentivate a prendere sufficientemente sul serio l'impegno necessario per conformarsi alla protezione dei dati.

Con l'entrata in vigore del RGPD, tutto ciò è cambiato radicalmente:

Con il RGPD incombono **sanzioni amministrative per importi fino a 20 milioni di euro o pari al 4% del fatturato mondiale totale annuo dell'esercizio precedente.**

Il quadro delle sanzioni pecuniarie è stato così notevolmente aumentato e standardizzato a livello UE. Il limite superiore "alternativo" della sanzione dipende da quale dei due valori è il più alto (20 milioni o 4% dei ricavi). In quale misura le competenti autorità di vigilanza faranno uso di questo "quadro sanzionatorio" e soprattutto con quale frequenza verranno imposte le sanzioni, è attualmente difficile da prevedere. In combinazione con il rischio per la reputazione già esistente, la previsione di sanzioni amministrative rappresenta già, comunque, un incentivo molto significativo a soddisfare i requisiti imposti dalla protezione di dati. Tali sanzioni possono riguardare non solo le grandi catene alberghiere, ma sono anche importanti per gli hotel di piccole e medie dimensioni e possono eventualmente incombere proprio su tali strutture alberghiere.

Inoltre, per i soggetti interessati dall'elaborazione dei dati esistono modi diversi per far rispettare i loro diritti in sede civile. Essi possono ottenere, per esempio, il divieto giuridico di alcuni atti e richiedere i danni in determinate circostanze. Soprattutto in Germania, in caso di violazione della protezione dei dati, incombono diffide con procedimenti giudiziari successivi da parte dei concorrenti. Solitamente, le sentenze del giudice competente nei confronti delle strutture alberghiere sono prontamente esecutive in Svizzera. Infine, le leggi nazionali degli Stati membri contengono anche ipotesi di reato per alcune violazioni della protezione dei dati.

2. Quando sarà applicabile alle imprese svizzere il RGPD?

Partendo dal presupposto delle drastiche conseguenze che incombono in caso di inosservanza del RGPD, si pone la questione di quali siano i soggetti interessati da tali direttive. Ciò può essere spiegato per mezzo di diverse configurazioni. Come dimostrano gli esempi qui sotto, il campo di applicazione del regolamento è volutamente inteso in modo molto ampio.

Il RGPD in particolare non viene applicato **solo per il trattamento dei dati che avviene all'interno dell'UE**. Inoltre, le regole **sono applicabili alle numerose aziende senza succursale nell'Unione europea**. È anche irrilevante se si tratti di dati di cittadini dell'UE o meno.

Pertanto, molte più aziende e organizzazioni del settore alberghiero svizzero sono interessate dalle nuove direttive rispetto ad altre norme UE. Non sorprende che molti non siano (ancora) consapevoli del fatto che il RGPD si applica anche a loro.

a. Hotel svizzeri con succursale nell'UE

Una prima configurazione riguarda i casi in cui a prima vista non sorprende che il RGPD richieda di essere applicato:

Le strutture alberghiere con sede in Svizzera devono rispettare il RGPD se dispongono di una succursale nell'UE e trattano dati personali nell'ambito delle attività di tale filiale.

Per succursale si intendono soprattutto le società affiliate. Se quindi una casa madre svizzera dispone di una società affiliata nell'UE che partecipa al trattamento dei dati della madre, per esempio trasmettendole i dati sulle prenotazioni ricevute, dovrà essere applicato il

RGPD anche all'ulteriore trattamento dei dati da parte della casa madre.

Si noti, tuttavia, che il concetto di "succursale" è inteso in senso ampio. Sono compresi anche semplici filiali, reparti o in generale "impianti fissi".

❶ Esempio:

Per questo, vengono presi in considerazione come succursali, ad esempio, anche gli hotel di un gruppo alberghiero nella UE e in linea di principio il RGPD è applicabile al trattamento dei dati eseguito in tale contesto.

b. Hotel svizzeri senza succursale nell'UE

Oltre ai casi sopra citati con succursale nell'UE, vi sono altre tre configurazioni che **includono nell'ambito di applicazione del RGPD anche le strutture alberghiere svizzere senza alcuna struttura nell'UE**. Questi casi illustrano che l'effetto del RGPD si estende ben oltre i confini UE. In particolare i primi due casi si riferiscono per una parte sostanziale a circostanze di fatto online e sono così di fondamentale importanza anche per le strutture alberghiere, dal momento che gran parte delle prenotazioni arrivano attraverso piattaforme di prenotazione internazionali (hotel.com, booking.com) oppure attraverso il sito web.

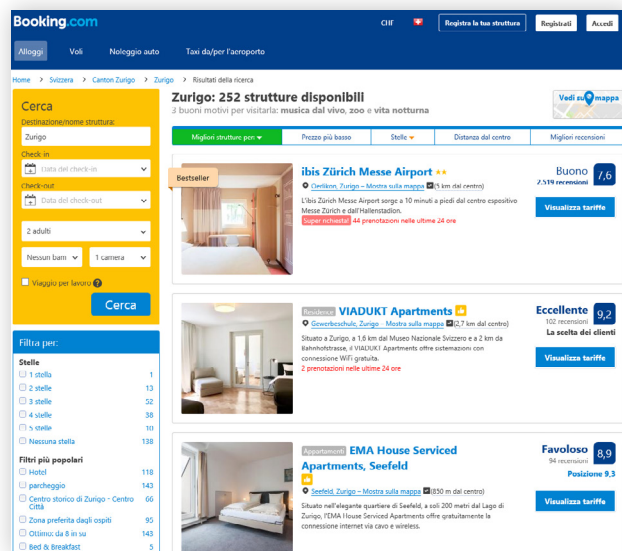
1. Offerta di beni o la prestazione di servizi ai suddetti interessati nell'UE

Alle direttive della legislazione europea sulla protezione dei dati sono sottoposte anche le strutture alberghiere svizzere che offrono i loro prodotti o servizi a ospiti nell'UE e che in tale contesto trattano informazioni personali.

Per "offrire" si intende per la verità solo "un'offerta palesemente intenzionale" a clienti dell'UE. Così, ad esempio, un hotel svizzero non dovrebbe quindi sottostare al RGPD solo per il fatto che in realtà è possibile anche alle persone nell'UE eseguire prenotazioni sul sito web dell'hotel. Tuttavia, per valutare se un'offerta è mirata (anche) a persone dell'UE, si tende a soddisfare dei criteri che possono essere interpretati in senso molto ampio in altri ambiti giuridici. Pertanto, è decisiva la questione se l'hotel si adoperi in modo mirato e consapevole per rivolgersi e attrarre potenziali clienti residenti nell'UE. Se le cose stanno così, l'offerta è proprio indirizzata a ospiti dell'UE e tali ospiti potranno appellarsi ai propri diritti previsti dal RGPD qualora l'hotel svizzero trattasse i loro dati in modo corrispondente. L'azione di "offrire" ai sensi del RGPD non si concretizza però solamente quando cittadini europei si rivolgono alla reception dell'hotel per eseguire una prenotazione.

❶ Esempi

Chi pubblica offerte su una piattaforma per prenotazioni come booking.com che si rivolge, tra gli altri, anche a paesi dell'Unione Europea, si rivolge quantomeno anche a ospiti dell'UE.



Fonte: booking.com (visitato l'11.6.2018)

Anche chi mette a disposizione dell'utente, sul proprio sito, una possibilità di opzione "proprio paese", si rivolge perlomeno anche alla clientela dei paesi

effettivamente citati. Nell'esempio di Svizzera Turismo, il RGPD è pertanto applicabile.

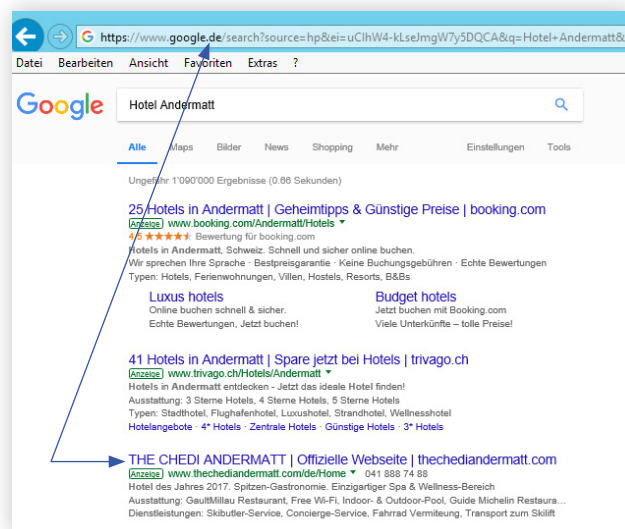


Fonte: <https://www.myswitzerland.com/it-ch/changecountry.html> (visitato l'11.6.2018)

Così, in particolare l'indicazione supplementare dei prezzi in euro, la presentazione del sito web nelle lingue dei paesi UE oppure l'indicazione dei costi di spedizione nei paesi membri UE per la spedizione di articoli di merchandising o di voucher degli hotel sono chiare indicazioni di un orientamento simile. Qualora venga gestita una pubblicità online per un'offerta rivolta in modo mirato a clienti UE (ovvero attraverso campagne AdWords opportunamente pianificate sul piano geografico), ciò sarebbe prova evidente del fatto che l'offerta reclamizzata deve rivolgersi a clienti del territorio corrispondente. In tal caso, pertanto, per il trattamento dei dati inerente all'offerta dovranno essere rispettate le regole del RGPD.

i Esempio:

Se dunque un soggetto riserva degli annunci su Google per le keyword "Albergo Andermatt" per la connessione a google.it, la sua offerta si rivolge anche ai clienti italiani. Così, in linea di principio, il RGPD è applicabile ai successivi offerenti.



Infine, il fatto che vengano comprese **anche le offerte a titolo gratuito** comporta un notevole ampliamento del campo di applicazione. In tal modo, anche i gestori di siti web di natura puramente informativa, come ad esempio i siti delle principali destinazioni e località turistiche ma anche delle più piccole strutture alberghiere, sottostanno al RGPD se il sito è rivolto (anche) a persone dell'Unione Europea. Criteri determinanti per valutare l'orientamento sono in tal caso, tra gli altri, le versioni linguistiche del sito web, il top-level domain oppure l'indicazione del prefisso internazionale. In particolare, ogni forma di marketing online mirato ai mercati UE è una prova evidente dell'orientamento.

2. Osservazione del comportamento delle persone nell'UE

Non solo l'azione di offrire, bensì anche quella di osservare semplicemente il comportamento delle persone nell'UE comporta l'applicabilità del RGPD.

Con questo, il regolamento si riferisce primariamente a circostanze di fatto su Internet. Qui sono compresi i processi di trattamento dei dati con i quali si intende seguire il comportamento delle persone nell'UE, principalmente per scopi pubblicitari.

Pertanto, il RGPD trova applicazione in linea di principio in tutti i metodi del cosiddetto user/customer-tracking, in particolare quei metodi che funzionano facendo ricorso ai cookie.

❶ Esempio:

Se, ad esempio, un hotel imposta sul proprio sito web degli strumenti di analisi per valutare le visite al sito e il comportamento degli utenti, come ad esempio Google Analytics, si dovrà tener conto dell'applicabilità del RGPD.

3. Incarico/mandato con imprese UE

Un'altra circostanza che ha come conseguenza che gli hotel svizzeri senza succursale nell'UE debbano sottostare al RGPD sono i cosiddetti **rapporti per il trattamento dei dati a contratto**. Ciò è rilevante se un hotel svizzero incarica un'altra azienda o terze parti a propria discrezione affinché elabori i propri dati (ad esempio, i dati dei dipendenti o dei clienti) per scopi propri della committente. Come mostra il seguente esempio, anche il caso contrario comporta che l'hotel svizzero venga compreso nel campo di applicazione del RGPD.

❶ Esempio:

Se pertanto un hotel svizzero utilizza i servizi di un provider di cloud con succursale nell'UE, ad esempio per la memorizzazione di dati personali, è applicabile il RGPD. Lo stesso vale per il caso inverso, se, ad esempio, un hotel svizzero elabora dati personali su incarico di un'azienda UE. Se l'elaborazione centralizzata dei dati di una catena alberghiera viene quindi effettuata, ad esempio, da parte di un'azienda in Svizzera, ma su incarico dei singoli hotel nell'UE appartenenti alla catena, le regole del RGPD dovranno essere rispettate.

III. Cosa è necessario fare, ora, nel trattamento dei dati personali ovvero dei dati degli ospiti?

Il RGPD ed anche la revisione in atto della legge federale sulla protezione dei dati portano con sé ampie innovazioni. È certamente probabile che la nuova legge svizzera sulla protezione dei dati (LPD) in diversi punti non andrà oltre i nuovi regolamenti UE. A causa però dell'ampio campo di applicazione del RGPD, come illustrato, solo pochissime imprese dell'industria alberghiera svizzera, se non nessuna, non sono da ciò comprese. Nei chiarimenti successivi, l'attenzione verrà quindi posta sulle direttive del RGPD già stabilite, in vigore dal 25 maggio 2018.

1. In linea di principio, il trattamento dei dati personali è vietato, a meno che ...

Punto centrale, dal punto di vista delle strutture alberghiere svizzere, è l'idea del cosiddetto **"divieto con riserva di autorizzazione"** prevista dal RGPD:

Quindi, in linea di principio, è vietato ogni trattamento di dati personali. Ciò che è ammesso, ad esempio, è il trattamento dei dati di ospiti o clienti solo quando una struttura alberghiera può richiamarsi ad un'autorizzazione di fatto, stando alla quale è a malapena ammesso il trattamento.

Simili autorizzazioni di fatto possibili sono in particolare, secondo il RGPD:

- **"Consenso"**: L'elaborazione dei dati è ammessa se si basa su un consenso efficace della persona interessata. I requisiti richiesti per un consenso valido,

efficace sotto il profilo giuridico, sono però sensibilmente aumentati e non corrispondono alla pratica imprenditoriale fin qui predominante in Svizzera in materia di consenso (si veda più avanti).

- **“Contratto”**: L’elaborazione dei dati può essere consentita se essa è necessaria per l’adempimento di un contratto con la persona interessata. Pertanto, un hotel potrà naturalmente sempre elaborare i dati degli ospiti nella misura in cui ciò è necessario per l’organizzazione e la contabilizzazione del soggiorno.
- **“Legge”**: Sono consentiti i trattamenti dei dati personali che sono necessari per l’adempimento di obblighi di legge (ad esempio, l’obbligo di conservazione e l’obbligo di segnalazione).
- **“Interesse prevalente”**: Infine, l’elaborazione dei dati può essere consentita se essa è necessaria per garantire un interesse legittimo della struttura alberghiera, purché l’interesse superi quello della persona interessata. Qui, tuttavia, in caso di interesse meramente economico all’esecuzione di interventi di marketing, è sempre necessaria un’accurata verifica nel singolo caso.

2. Principi fondamentali di ogni legittima elaborazione dei dati

La mera presenza di un’autorizzazione di fatto non conduce ancora, comunque, al fatto che un’elaborazione dei dati soddisfi le direttive del RGPD. Dovranno piuttosto essere rispettati in particolare anche i cosiddetti principi per il trattamento dei dati. Con questo, per principi fondamentali di una legittima elaborazione dei dati si intendono i principi che sono già previsti nel diritto UE e svizzero in vigore. Questi sono stati recentemente rafforzati e soprattutto la loro violazione è passibile di sanzioni.

Da sottolineare sono in particolare i seguenti principi:

- **Principio di limitazione delle finalità**: I dati personali possono essere raccolti ed elaborati solo per finalità chiaramente definite.
- **Principio di trasparenza**: L’elaborazione dei dati e le finalità con essa perseguite devono essere

comprensibili alla persona interessata dal momento della loro raccolta e in qualsiasi momento successivo.

- **Minimizzazione dei dati**: Possono essere raccolti esclusivamente i dati personali necessari per la finalità del trattamento determinata. Non possono essere rilevati dati per scorta ed ulteriormente elaborati.
- **Limite alla memorizzazione**: I dati personali possono essere memorizzati solo per il tempo necessario per la finalità del trattamento determinata. Una volta raggiunta la finalità, i dati devono essere cancellati.

3. Nuova ed ampia “diligenza dovuta” nella gestione dei dati

Il RGPD impone inoltre alle strutture alberghiere molteplici nuovi obblighi formali.

Si sottolinea quanto segue:

- **Registro delle attività di trattamento**: Da poco, ogni struttura alberghiera che elabori dati personali deve tenere un registro di tutti i rilevanti trattamenti dei dati. In tale registro, per ogni adeguato processo di elaborazione, deve essere documentata e descritta dettagliatamente una serie di informazioni (ad esempio, la finalità, responsabilità, il tipo di dati, i rischi specifici, ecc.).
- **Obbligo di prova**: Il RGPD impone in modo esplicito che i responsabili della elaborazione dei dati siano in grado di provare in qualsiasi momento il rispetto dei principi del trattamento dei dati. A questo serve, tra gli altri, il registro per il trattamento dei dati
- **Valutazione d’impatto sulla protezione dei dati**: In caso di trattamento dei dati che presumibilmente possono comportare un alto rischio per l’interessato, deve essere eseguita e documentata una valutazione di tale impatto. Ciò dovrà essere provato in particolare in caso di utilizzo di nuove tecnologie e di impiego di nuove forme di processi di trattamento dei dati.
- **“Data Breach Notifications”**: Eventuali violazioni

delle direttive del RGPD, in particolare l'abuso e il furto di dati, devono essere denunciate, in determinate condizioni, alle autorità di vigilanza e alle persone interessate.

- **Privacy by Design / by Default:** Il trattamento dei dati deve essere sviluppato in modo tale da garantire il rispetto della protezione dei dati e l'esercizio dei diritti dell'interessato in qualsiasi momento (informazione, cancellazione, correzione) (privacy by design). Inoltre, ogni elaborazione dei dati deve essere sviluppata in modo tale da lasciare le impostazioni predefinite che garantiscano maggiormente la protezione dei dati (privacy by default).
- **Nomina di un rappresentante:** Le strutture alberghiere senza succursale nell'UE devono nominarvi, di regola, un rappresentante.

4. Quali diritti hanno le persone i cui dati vengono elaborati ("Diritti dell'interessato")

Una elaborazione dei dati legittima impone che le persone i cui dati vengono elaborati possano seguire, in qualsiasi momento, quali dati che li riguardano vengono elaborati e in che modo. Il RGPD prevede pertanto i cosiddetti diritti dell'interessato. Gran parte dei diritti erano già previsti in linea di principio nel diritto finora in vigore, tuttavia i diritti dell'interessato sono stati ampliati e adattati a più riprese.

La persona interessata ha in particolare i seguenti diritti. Potrà farli valere in qualsiasi momento.

- **Diritto all'informazione:** Le persone interessate possono richiedere in qualsiasi momento alle strutture alberghiere informazioni sull'elaborazione dei dati che li riguardano.
- **Diritto di rettifica:** Oltre all'obbligo di fondo dell'azienda che elabora i dati ad adottare misure per garantire la correttezza dei dati, le persone interessate possono richiedere, in qualsiasi momento, l'immediata correzione di dati non corretti.
- **Diritto alla cancellazione e all'opposizione:** Le persone interessate possono, in determinate condizioni, opporsi all'esecuzione dell'elaborazione dei

dati e chiedere la cancellazione dei dati.

- **Portabilità dei dati:** Secondo il RGPD, i dati registrati devono essere elaborati in modo tale da poter essere rilasciati in qualsiasi momento alla persona interessata in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

IV. Direttive centrali per l'industria alberghiera

La maggior parte degli hotel eseguono regolarmente elaborazioni di dati che sono compresi nel campo di applicazione del RGPD (si veda qui sopra, a riguardo), anche se l'elaborazione avviene in Svizzera. Di conseguenza, tali elaborazioni di dati devono essere verificate nell'ottica dell'adempimento dei requisiti del RGPD, ed eventualmente adattate. Il RGPD è in vigore dal 25 maggio 2018. Di seguito vengono esaminati alcuni ambiti centrali per l'industria alberghiera ed illustrate le problematiche essenziali.

1. Trasparenza dell'elaborazione dei dati

a. Se i dati vengono raccolti direttamente dai vostri ospiti / partner commerciali

Primo passaggio di ogni processo di elaborazione dei dati è la raccolta ovvero acquisizione dei dati.

Secondo il RGPD, sussiste il dovere, nell'acquisire dati personali, di mettere a disposizione in modo attivo, dunque spontaneo, ampie informazioni circa il trattamento dei dati previsto.

L'elenco delle informazioni prescritte per legge è stato fortemente ampliato. Vengono richieste informazioni

“facilmente comprensibili” e “precise” sui seguenti punti:

1. Nome e dati di contatto del responsabile ed eventualmente del suo rappresentante
2. Dati di contatto dell'eventuale responsabile della protezione dei dati
3. Finalità e fondamento giuridico dell'elaborazione dei dati
4. L'eventuale interesse legittimo al trattamento dei dati
5. Eventuale destinatario o categoria di destinatari dei dati personali
6. L'eventuale intenzione di trasmettere i dati a stati terzi o ad un'organizzazione internazionale
7. Ulteriori informazioni che siano necessarie a garantire un trattamento corretto e trasparente
8. Durata della memorizzazione dei dati ovvero criteri per stabilirne la durata
9. Esistenza di diritti dell'interessato, come informazione, correzione, cancellazione, blocco, diritto all'opposizione o trasferimento dei dati
10. Diritto di revoca in caso di trattamento dei dati basato sul consenso
11. Esistenza del diritto di ricorso presso l'autorità di vigilanza
12. Eventualmente, se la fornitura dei dati è prevista per legge o per contratto o se è necessaria per la stipula del contratto
13. Esistenza di un processo decisionale automatico compreso il profiling nonché informazioni significative sulla logica e la portata coinvolte e gli effetti che si intende ottenere con un trattamento del genere per la persona interessata.

Tali informazioni devono essere ben visibili ed accessibili soprattutto là dove vengono acquisite le informazioni personali.

Ciò riguarda, in particolare, tutti i moduli di contatto, prenotazione o registrazione. Le strutture alberghiere devono pertanto creare delle informative sulla protezione dei dati che contengano le informazioni obbligatorie, oppure rivedere le informative sulla protezione dei dati già disponibili. Tali informative sulla protezione

dei dati devono infine essere facilmente reperibili e accessibili in qualsiasi momento, in particolare sui siti.

❶ Esempio:

Qualora un sito web di un hotel metta a disposizione degli ospiti o dei potenziali clienti un modulo di contatto, la nota o il link all'informativa sulla protezione dei dati deve essere inclusa prima o nei pressi del pulsante “Invia”. Ciò garantirà che le informazioni per gli ospiti ed i potenziali clienti siano accessibili e facili da trovare.

Ma anche in caso di registrazione di dati che non avvenga attraverso un sistema elettronico, ad esempio nel caso di moduli di iscrizione, schede di CRM o cedole di partecipazione a lotterie, deve essere garantito che le informazioni siano disponibili per le persone interessate (ad esempio, stampate sul retro di una scheda di CRM o della scheda di iscrizione).

Per soddisfare gli obblighi di notifica previsti per legge, le strutture alberghiere utilizzano in genere un modulo completo per raccogliere contemporaneamente, oltre alle informazioni legalmente obbligatorie per la notifica, altri dati sugli ospiti. È da notare che, anche in tale contesto, devono essere soddisfatti i requisiti di informazione. Qui, l'ospite dovrà essere informato in modo chiaro quali informazioni sono rilevate per l'obbligo di notifica previsto dalla legge (ad esempio, contrassegnandole con un asterisco) e quali altre informazioni vengono rilevate in aggiunta. Per questi due casi, si distinguono anche le corrispondenti autorizzazioni di fatto, cosa che a sua volta si ripercuote sulle informazioni necessarie.

b. Se i dati vengono acquisiti da fonti terze

Anche acquisendo dati “provenienti da fonti terze” sussiste l'obbligo di informazione e devono essere fornite le stesse ampie informazioni - con certe deroghe -.

Con l'acquisizione da fonti terze si intendono i casi in cui i dati non sono raccolti presso gli interessati (ad esempio gli ospiti), bensì, per esempio, da terzi o da fonti disponibili al pubblico.

❶ Esempio:

Tali acquisizioni indirette sono quelle che ad esempio avvengono nell'industria alberghiera quando un hotel richiede ad un impianto di funivia i dati di contatto delle persone che hanno acquistato uno skipass, per sottoporre a questi potenziali clienti delle offerte per un pernottamento. Altra acquisizione da fonte terza è quella effettuata con i dati degli ospiti raccolti attraverso portali di prenotazione come boking.com e che sono stati inviati all'hotel che è stato riservato. L'hotel dovrà pertanto informare l'ospite, al momento della presa di contatto, quali dati ha ricevuto e come verranno utilizzati.

2. Consenso

Ogni elaborazione di dati personali deve basarsi su una cosiddetta autorizzazione di fatto, altrimenti sarà vietata ai sensi del RGPD. Il consenso della persona interessata rappresenta una importantissima autorizzazione di fatto. I requisiti per la validità di un consenso del genere sono stati tuttavia sensibilmente ampliati con il RGPD.

Perché un consenso sia valido, esso deve essere dato volontariamente, in particolare sulla base di sufficienti informazioni preventive e in forma inequivocabile.

I requisiti ampliati valgono anche quando le persone interessate hanno dato il consenso prima dell'entrata in vigore del RGPD. In altre parole, anche i "consensi pregressi" sono validi solo se soddisfano i requisiti del RGPD.

a. Volontà libera e divieto di collegamento

Uno dei requisiti più importanti è rappresentato dalla volontà libera del consenso. La volontà libera può mancare se esiste un chiaro squilibrio tra le prestazioni che spettano alla persona interessata in virtù di un contratto e le elaborazioni di dati cui viene dato il consenso nel quadro del contratto.

Particolarmente importante è la questione di quando vige il cosiddetto **divieto di collegamento**. Secondo tale divieto, non è permesso vincolare l'esecuzione di un contratto al consenso ad ulteriori trattamenti di dati. Non si intendono, qui, trattamento dei dati che siano necessari all'esecuzione di un contratto, bensì principalmente l'utilizzo di dati per finalità pubblicitarie.

❶ Esempio:

Nell'esempio sopra citato, ciò significherebbe che l'impianto di funivia non dovrebbe subordinare l'emissione dello skipass al consenso del cliente alla trasmissione dei propri dati all'hotel.

Allo stato attuale, è certo che collegamenti del genere possono essere problematici. Finché non viene stabilita una prassi da parte delle autorità di vigilanza, pratiche simili sono rischiose e dovrebbero essere evitate oppure dovrebbe essere offerta una possibilità alternativa alle persone interessate.

b. Caselle preselezionate

I consensi sono validi solo se vengono espressi attraverso un chiaro atto confermativo.

Il silenzio o l'inattività dell'interessato pertanto non sono sufficienti.

❶ Esempio:

Se nel modulo di prenotazione sul sito web dell'hotel la casella per l'autorizzazione all'invio di newsletter è già preselezionata, non siamo in presenza di un consenso

valido. L'ospite deve invece barrare autonomamente la casella con un clic per rendere efficace il proprio consenso.

3. Passaggio di dati

a. Informazioni generali

All'interno di catene alberghiere o di associazioni di hotel in gruppi ci è un forte interesse al passaggio di dati tra le parti in causa.

Il passaggio di dati a terzi, tuttavia, è una "divulgazione tramite trasmissione" e quindi è un'elaborazione dei dati che è soggetta ai requisiti del RGPD se riguarda dati personali.

Esiste anche qui, pertanto, l'obbligo all'informazione. Il passaggio al proprio interno deve essere fatto in modo trasparente e se fatto verso altri deve essere chiarito per quali finalità viene eseguito. Inoltre, il soggetto che esegue la trasmissione dei dati deve essere in grado di dimostrare che è stata data un'autorizzazione di fatto (ad esempio, un consenso).

Viene spesso trascurato il fatto che anche la **concessione dell'accesso** ai dati è considerata una trasmissione di dati.

❶ Esempio:

Qualora alcune catene alberghiere o determinati hotel riuniti in associazione utilizzassero un CRM centrale comune, si è già in presenza di un passaggio di dati a terzi ai sensi del RGPD.

b. "Parti terze"

In questo scenario, è particolarmente importante stabilire chi siano le parti terze.

Le strutture alberghiere spesso non sono consapevoli del fatto che anche gli altri hotel della stessa catena alberghiera, le società dello stesso gruppo o membri (giuridicamente indipendenti) di un'associazione sono terze parti.

Pertanto, anche in caso di **trasmissione di dati interna al gruppo**, le regole del regolamento generale sulla protezione dei dati devono essere osservate, dunque se a una filiale o consociata viene consentito l'accesso a dati personali.

c. Trattamento dei dati su commissione

Una forma particolare di passaggio di dati si verifica nell'ambito del cosiddetto trattamento dei dati su commissione.

Si intendono quei casi in cui un'altra azienda viene incaricata di modificare i propri dati (ad esempio, i dati di dipendenti, ospiti o clienti) per le finalità del committente.

Nella prassi aziendale, tali configurazioni si presentano in genere molto spesso e in modo significativo.

❶ Esempio:

Nell'industria alberghiera, una configurazione simile si presenta solitamente nell'ambito dell'utilizzo di soluzioni CRM

basate su cloud, con il coinvolgimento di fornitori di servizi terzi sul sito web dell'hotel (ad esempio, tool di analisi web, funzioni chat ecc.) ma, eventualmente, anche in occasione di collaborazioni con un negozio sportivo locale. Configurazioni di trattamento dei dati su commissione possono anche presentarsi in particolare se tutti gli hotel di una catena alberghiera incaricano un determinato hotel oppure una società di servizi di preparare e gestire un sistema CRM centrale per l'elaborazione dei dati degli ospiti.

Diffusi casi di applicazione emergono quando viene fatto ricorso ai seguenti servizi o programmi:

- Mailchimp per l'invio di newsletter
- Google Analytics per l'analisi del web
- Provider di cloud per la memorizzazione di dati
- Microsoft 365 (soluzione cloud)
- Chatlio (funzioni chat sul sito web)
- Social Monitoring Tools
- Salesforce / Microsoft Dynamics (sistemi di CRM)
- Webhoster

Qui è fondamentale come il RGPD richieda in modo esplicito la stipula di un contratto scritto, che può avvenire anche in un "formato elettronico". Nel contratto, il committente deve farsi concedere diritti di dare le direttive e di controllo. In altre parole, il soggetto incaricato deve in particolare essere obbligato ad elaborare i dati solo secondo le direttive del committente. Importante contenuto del contratto è anche la questione se il soggetto incaricato possa o meno ricorrere a terzi (**aziende in subappalto**). Poiché, secondo il RGPD, ciò può essergli concesso solamente con l'approvazione del committente.

❶ Esempio:

Se l'hotel sfrutta il servizio di "Google Analytics" per l'analisi dell'utilizzo del sito web, Google deve essere vincolato contrattualmente a elaborare i dati "secondo le direttive impartite". Per questo, Google metterà a disposizione una proposta

contrattuale la cui legittimità ai sensi del RGPD non è tuttavia ancora stata chiarita definitivamente.

Il committente può "affidare a terzi" l'elaborazione di dati solo ad aziende che con l'implementazione di misure tecnico-organizzative possano garantire l'elaborazione in sintonia con il RGPD. Il committente rimane in ogni caso responsabile del rispetto delle direttive sulla legge per la protezione dei dati, anche con l'impiego di terzi. Tuttavia, anche al responsabile del trattamento dei dati su commissione spettano numerosi obblighi ai sensi del RGPD. Inoltre, contro tale soggetto possono essere comminate sanzioni.

d. Trasmissione all'estero

Particolare attenzione richiede la questione relativa a quale paese sia destinatario dei dati trasmessi. Soprattutto in caso di trasmissione negli Stati Uniti è richiesta attenzione.

Poiché gli Stati Uniti vengono considerati un paese senza adeguato livello di protezione dei dati, motivo per cui in linea di principio non è ammessa una trasmissione di dati senza particolari misure precauzionali.

Nel quadro del cosiddetto accordo sul "privacy-shield", le imprese statunitensi possono però acquisire una **certificazione** che conferma che le imprese certificate soddisfano spontaneamente certi requisiti legati alla legge sulla protezione dei dati e pertanto garantiscono un adeguato livello di protezione della privacy. In tali casi, la trasmissione viene certamente concessa in sé, tuttavia devono essere osservati ulteriori requisiti. Nel passaggio di dati ad aziende statunitensi senza certificazione, sono necessarie "garanzie" speciali, come la stipula di cosiddette **clausole standard di protezione dei dati**. Qualora mancassero adeguate garanzie, la trasmissione a paesi terzi non è ammessa.

❶ Esempio:

Un hotel che imposta sul proprio sito web il cosiddetto remarketing pixel di Facebook per consentire un marketing personalizzato nelle reti social, trasmette, così, dati personali a Facebook, con sede negli Stati Uniti. Facebook è un'impresa certificata ai sensi del "privacy shield", per cui non sono necessarie garanzie supplementari. Rimane ancora poco chiaro, e quindi problematico, come possa essere stipulato un sufficiente contratto di trattamento dei dati su commissione con Facebook.

4. Sistemi CRM

L'entrata in vigore del RGPD ha portato con sé grandi sfide anche per il trattamento dei dati nell'ambito di sistemi per la gestione dei clienti (CRM). Senso e finalità di tali sistemi sono, tra gli altri, la memorizzazione centralizzata di tutti i processi commerciali rilevanti con i singoli ospiti.

Proprio questo ricongiungimento ovvero collegamento di una vasta gamma di dati da fonti diverse è tuttavia problematico sotto il profilo della protezione dei dati.

a. Trasparenza e legittimità

Sulla base dell'obbligo di informazione e trasparenza, gli ospiti devono essere informati in particolare del collegamento e della memorizzazione a livello centralizzato dei loro dati. A ciò connesso è anche il problema della "causa di giustificazione". Poiché per la memorizzazione dei dati di prenotazione può senz'altro essere adatta l'autorizzazione di fatto "contratto", per il collegamento dei dati sarà tuttavia per lo più necessario un consenso dell'ospite. Tale consenso sarà tuttavia efficace se viene concesso dall'ospite sulla base di

sufficienti informazioni relative al trattamento dei dati. È pertanto richiesta una chiara ed esaustiva informazione dell'ospite interessato in tutti e due gli aspetti.

❷ Esempio:

Qualora, nel sito web dell'hotel, fosse possibile anche prenotare una stanza o un servizio, l'ospite dovrà essere informato direttamente dal modulo per l'inserimento dei propri dati del fatto che i propri dati verranno memorizzati in una banca dati centralizzata e collegati ad altre informazioni, come ad esempio lamentele relative a precedenti soggiorni. L'hotel dovrà raccogliere contemporaneamente il consenso dell'ospite.

Punto centrale, a riguardo, è che anche i consensi dati dagli ospiti (compresi data e formulazione della dichiarazione e delle informazioni) siano documentati e possano essere recuperati rapidamente, se necessario.

b. Finalità vincolata e modifica delle finalità

In tale contesto, è necessario prestare particolare attenzione al fatto che i dati disponibili non vengano elaborati per nuove finalità che non siano più previste dalla finalità originariamente indicata. Ciò può essere problematico in particolare per i "dati vecchi".

Qualora i dati personali di una banca dati venissero trasferiti ad un'altra, si dovrà sempre considerare se non si verifichi un cambiamento di finalità.

Se ciò accadesse, l'ospite o cliente interessato dovrà esserne informato e dovrà prestare il proprio consenso al trattamento dei dati per la nuova finalità.

Lo stesso problema si pone quando, dai dati a disposizione, devono essere derivate nuove nozioni. Nelle **analisi CRM o big data** di questo tipo, è difficile definire già in partenza quali reali nozioni vengano acquisite in ultima analisi. Quindi, è obbligatoria una particolare attenzione nella formulazione delle informazioni, in particolare della finalità del trattamento dei dati.

❶ Esempio:

Se l'hotel dell'esempio precedente nella propria informativa sulla protezione dei dati ha informato che i dati verranno valutati con la finalità di assegnare gli ospiti ad un determinato target o segmento di ospiti in modo da poter loro sottoporre una pubblicità personalizzata, non potrà estendere l'analisi anche per stabilire un prezzo personalizzato. In un secondo momento, tuttavia, dall'analisi emergeranno eventualmente anche nozioni relative al prezzo in modo che vi sarebbe già una modifica della finalità.

Resta ancora in gran parte poco chiaro in che modo tali analisi possano essere conciliate con il principio della **parsimonia dei dati**. Ma è proprio il generare e l'analizzare il numero più alto possibile di dati che determina la forza espressiva dei risultati delle analisi. Il RGPD richiede sempre, tuttavia, che già in fase di raccolta venga specificato per quanto tempo i dati rimangono memorizzati oppure, "qualora ciò non fosse possibile", quali siano i criteri per stabilire tale durata. Le imprese devono pertanto definire in ogni caso anche per il sistema CRM un **piano per la cancellazione o conservazione** dei dati personali.

c. Diritti di accesso e trasmissione

Per l'impiego di sistemi CRM conformi alla tutela dei dati è particolarmente importante anche il regolamento dei diritti di accesso.

È necessario assicurarsi che i dipendenti possano accedere esclusivamente ai dati che sono necessari per l'assolvimento dei loro compiti.

Questo **"principio del need-to-know"** deve essere messo in atto attraverso un piano di autorizzazioni nel quale vengano stabilite regole di accesso per i singoli utenti o gruppi di utenti.

Oltre a questo aspetto interno all'azienda, emergono problematiche fondamentali già dal diverso tipo di sistema CRM selezionato. Poiché gran parte dei programmi si basa su una soluzione cloud e i provider o i servizi di hosting si trovano all'estero. In tal caso, devono comunque essere rispettate le direttive per la **trasmissione all'estero** e per il **trattamento dei dati su commissione**.

5. Marketing per e-mail

Per il recapito di e-mail promozionali e in particolare l'invio di una newsletter, emergono ulteriori problematiche dall'interazione tra il diritto alla protezione dei dati e il diritto alla concorrenza. Poiché da un lato vengono regolarmente elaborati dati personali e dall'altro le leggi nazionali prevedono stringenti regole per la tutela contro lo "spam".

Una particolarità svizzera consiste nel fatto che le violazioni contro "l'articolo sullo spam" sono già oggi **sanzionate penalmente**.

Su questo scenario, le strutture alberghiere dovrebbero prestare particolare attenzione al rispetto delle direttive di legge quando eseguono marketing per e-mail.

a. Consenso ("opt-in")

Per la legalità di e-mail promozionali, di regola è richiesto un **consenso** del destinatario.

Come già illustrato, un consenso sarà valido solamente se viene dato in base a sufficienti informazioni relative al trattamento dei dati legato all'invio. Anche tali informazioni devono pertanto essere contenute nell'**informativa sulla protezione dei dati** e poste in evidenza nell'ambito del processo di registrazione.

Si pone inoltre la questione relativa a quale forma possa avere il consenso che deve essere raccolto dai potenziali clienti. È stato già illustrato che secondo il RGPD **le caselle preselezionate** non sono sufficienti per raccogliere un consenso valido da parte del potenziale cliente. Inoltre, si consiglia vivamente alle strutture alberghiere di impostare la cosiddetta **procedura di "doppio opt-in"**:

1. Per questo, nell'ambito del processo di iscrizione, viene richiesto un primo "opt-in" per il recapito della newsletter all'indirizzo e-mail indicato.
2. Immediatamente dopo, in un secondo passaggio e prima del recapito della newsletter per la prima volta, viene inviata una e-mail con l'invito a confermare l'iscrizione con un click su un link corrispondente (secondo "opt-in").

Sullo sfondo di tale procedura vi è il problema che non è praticamente possibile provare giuridicamente il consenso senza il "secondo opt-in".

❗ Esempio:

Nell'esempio della newsletter dello Swiss Diamond Hotel, il passaggio 1 ha il seguente aspetto:

Il passaggio 2 ai sensi del doppio opt-in viene messo in atto come segue:

b. Passaggio di dati a terzi e trasmissione all'estero

Per l'invio della newsletter, le strutture alberghiere ricorrono regolarmente a strumenti di terzi. A seconda della reale organizzazione, ciò può comportare la presenza di un **rapporto di trattamento dei dati su commissione**. In tal caso, devono essere rispettati i requisiti già illustrati, quindi deve essere stipulato un accordo sui diritti di impartire direttive e sui diritti di controllo. Si aggiunge inoltre il fatto che diversi provider, come ad esempio MailChimp, hanno la propria sede negli Stati Uniti e che i dati vengono memorizzati in questi server. Ciò ha come conseguenza il fatto che devono essere rispettati i requisiti per la **trasmissione all'estero** (soprattutto l'obbligo di informazione e le garanzie).

Vi sono poi ulteriori direttive se l'invio della newsletter stessa avviene oltre i confini. Se i potenziali clienti

stranieri sono liberi di registrarsi, dovranno essere rispettate, eventualmente, anche le **regole nazionali degli altri stati**. Ciò dipende, in particolare, se il sito web e l'offerta della newsletter sono "mirati" a ospiti in tale paese, cosa relativamente molto probabile. Valgono così essenzialmente gli stessi criteri visti nella questione dell'applicabilità del RGPD agli hotel svizzeri senza succursale nell'UE (si veda sopra).

Di conseguenza, anche le newsletter degli hotel svizzeri sono sottoposte regolarmente alle regole del diritto tedesco.

Nel diritto tedesco, basta una sola mail promozionale senza consenso per ricevere una diffida come spammer con la quale vengono rivendicati diritti di cessazione e richiesto il risarcimento delle spese legali. Nell'organizzazione del processo legato alle newsletter non possono pertanto essere trascurate le regole del RGPD e neppure le ulteriori norme legali straniere.

6. Analisi del web / tracking

Nell'ambito del piano di marketing, naturalmente anche il sito web della struttura alberghiera gioca un ruolo centrale. Per valutare le visite al sito web viene fatto ricorso a servizi quali Google Analytics.

Sotto il profilo della legge sulla protezione dei dati, in tale contesto si devono rispettare diversi requisiti già illustrati in precedenza. Spesso, come nell'esempio di Google Analytics, si verifica una trasmissione dei dati a terzi che hanno sede negli Stati Uniti.

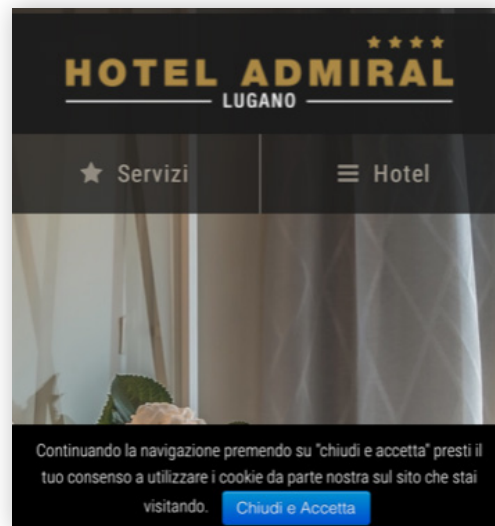
Pertanto, devono essere rispettati i requisiti per il trattamento dei dati su commissione e per la trasmissione dei dati verso paesi terzi. Inoltre, nell'informativa sulla protezione dei dati deve essere indicato l'utilizzo di tali

servizi - per soddisfare l'obbligo di informazione - e spiegato il trattamento dei dati a ciò collegato.

Notoriamente, gli strumenti di analisi si basano regolarmente sull'**impiego di cookie** o di tecnologie simili, attraverso le quali può essere seguito il comportamento di navigazione dell'utente su più pagine. Già in virtù del diritto UE in vigore, gli utenti devono essere informati sull'utilizzo di cookie e deve venir loro chiesto il consenso per questo. Nella pratica, tale requisito attualmente viene messo in atto prioritariamente attraverso la diffusione di **banner dei cookie**, che vengono mandati in sovrapposizione accedendo ad un sito web.

❶ Esempio:

Come esempio, l'hotel Admiral Lugano ha attualmente attivato il seguente banner sul proprio sito web:



Fonte: <http://www.luganohoteladmiral.ch/> (visitato l'11.6.2018)

Si osservi, tuttavia, che nell'UE è in progetto una stretta regolamentazione per i cookie che dovrà essere applicata in via complementare rispetto al RGPD. Attualmente, il reale contenuto di tale cosiddetto **regolamento sulla vita privata e le comunicazioni elettroniche** non è ancora stato stabilito. Tuttavia, si prospetta lo scenario secondo cui in futuro neanche gli attuali banner dei cookie saranno più sufficienti. Sarà pertanto necessario tener monitorati i successivi sviluppi.

7. Monitoring dei social media

Gran parte delle strutture alberghiere integra il proprio piano di marketing anche con una presenza sulle piattaforme dei social media di loro interesse. Su tali piattaforme, migliaia di utenti si esprimono ogni giorno su prodotti, servizi e fornitori. Per molte imprese è pertanto prassi corrente osservare ed analizzare, oltre ai media classici, anche i social media.

Sia nel diritto svizzero che in quello tedesco, ad esempio, vi erano fino ad oggi regole speciali per il trattamento dei dati resi accessibili al pubblico. Regolamenti paragonabili non sono più presenti nel RGPD, motivo per cui la situazione legale anche in tale ambito si è notevolmente inasprita. Le pratiche del monitoring dei social media, già problematiche ai sensi del diritto fino ad oggi in vigore, presentano pertanto notevoli rischi.

Particolari criticità si presentano già per l'assolvimento dell'**obbligo di informazione**. Esso subentra anche se i dati non vengono raccolti presso la stessa persona interessata.

Sulle piattaforme, si pone tuttavia la questione di come queste informazioni possono essere fornite all'interessato in forma sufficiente.

Almeno con riferimento ai dati che un utente rilascia in un profilo di una struttura alberghiera (ad esempio, scrivendo un post), è immaginabile un collocamento in una rubrica a parte del profilo. Diversamente, ad esempio, dai moduli di contatto su un sito web, tali informazioni però non possono di regola essere collegate con un link direttamente nel punto dove l'utente pone il proprio post. Pertanto, allo stato attuale, si pone la questione se le autorità di vigilanza considerino sufficiente tale prassi.

❶ Esempio:

Dunque, se il Tschuggen Grand Hotel sul proprio profilo Facebook alla rubrica "Informazioni" collegasse oltre a "Note

legali" alcune informazioni supplementari sulla protezione dei dati, rimane il dubbio se tali informazioni siano sufficientemente trasparenti.

The screenshot shows the Facebook profile of Tschuggen Grand Hotel. The profile name is 'Tschuggen Grand Hotel' with the handle '@tschuggengrandhotel'. The cover photo is a scenic view of a mountain valley. The main content area includes a map showing the hotel's location in Arosa, Switzerland, with the address 'Tschuggenforweg 1, Arosa' and phone number '081 378 99 99'. Below the map, there is a section titled 'INFORMAZIONI AZIENDALI' (Company Information) which includes details about parking, price range (€€€€), contact information (info@tschuggen.ch, http://www.tschuggen.ch), and a list of services such as 'Informazioni' (Information), 'Impressum', 'Informazioni generali' (General Information), and 'Trasporti pubblici' (Public Transport).

Fonte: https://www.facebook.com/pg/tschuggengrandhotel/about/?ref=page_internal (visitato il 11.6.2018)

Con tali presupposti, le informazioni obbligatorie dovrebbero essere poste alla conoscenza di ciascun utente in un secondo momento. Ciò vale ancora di più nel caso di raccolta di dati che gli utenti hanno pubblicato in altri ambiti pubblicamente accessibili. In tali casi, si pone comunque la questione se l'azienda possa richiamarsi ad un'autorizzazione di fatto. Di regola, un'autorizzazione di fatto manca. Per quel che riguarda la raccolta di dati in ambiti non pubblici, essa sarà sempre inammissibile, come accade già in virtù del diritto in vigore.

❶ Esempi:

Se un utente pubblica un post sul profilo Facebook pubblico di un hotel con una domanda su un'offerta corrente, la domanda potrà ricevere una risposta e in linea di principio il servizio può essere reso.

Inammissibile sarebbe però il collegamento dei dati nel sistema CRM, perché per questo sarebbe necessario un consenso informato dell'utente.

Se l'utente pubblica una foto e i propri commenti sul suo soggiorno in un hotel sul proprio profilo Facebook non pubblico, le aziende non potranno né rispondere al post né trattare altrimenti i dati. Perché anche qui sarebbe necessario il consenso informato.

8. Giochi a premi

Un modo molto diffuso per integrare le attività di marketing è offrire giochi a premi. Nello svolgimento dei giochi a premi vengono regolarmente elaborati anche dati personali. A tal riguardo, vi è di conseguenza l'obbligo di informazione nei confronti dei partecipanti. Tale obbligo di informazione viene solitamente rispettato con le condizioni di partecipazione. Sotto il profilo dei contenuti, le condizioni di partecipazione devono soddisfare i requisiti previsti dal RGPD, come illustrato in precedenza.

Oltre all'obbligo di informazione nei confronti dei partecipanti, è necessario ottenere anche un adeguato consenso giuridicamente efficace. Tale consenso dovrà a sua volta soddisfare i requisiti del RGPD. A tal riguardo, le caselle preselezionate sono inammissibili anche per i giochi a premi.

Nello svolgimento di giochi a premi è di fondamentale importanza il cosiddetto divieto di collegamento. Era prassi comune il fatto che partecipando al gioco a premi venisse collegato anche il consenso a ricevere newsletter e il consenso all'esecuzione di analisi ed elaborazione dei dati di utilizzo per finalità promozionali. A causa del divieto di collegamento, non è ammesso il collegamento della partecipazione al gioco a premi con il consenso alla newsletter. Per la newsletter deve quindi essere raccolto un consenso a parte dalla persona interessata.

i Esempio:

Sulla pagina Facebook dell'hotel viene pubblicato un gioco a premi con il quale

un giocatore può vincere un pernottamento. Per la partecipazione al gioco a premi, il partecipante deve accettare le condizioni di partecipazione e registrarsi alla newsletter. Tale procedura dell'hotel violerebbe il divieto di collegamento e sarebbe pertanto inammissibile.

9. WLAN dell'hotel

La maggior parte delle strutture alberghiere mette a disposizione dei propri ospiti una connessione WLAN. Anche in tale contesto vengono elaborati dati personali. Ciò accade, in particolare, quando viene registrato l'utilizzo ma anche durante l'utilizzo dell'accesso. Da una parte, può trattarsi dell'indirizzo IP e dall'altra dei corrispondenti dati di log-in delle persone interessate. Così sussiste, nei confronti degli ospiti e ai sensi del RGPD, un obbligo di informazione. Nella prassi, ciò viene in parte messo in atto per il fatto che gli ospiti devono effettuare un log-in per utilizzare la rete WLAN. Alla pagina di log-in gli ospiti vengono informati sulla nota relativa alla protezione dei dati. Inoltre, l'elaborazione dei dati deve fare riferimento ad un'autorizzazione di fatto (ad esempio un contratto o un consenso). Oltre alle informazioni complete sull'elaborazione di dati connessa all'utilizzo dell'accesso, è necessario fare attenzione affinché si verifichino esclusivamente le elaborazioni di dati che sono necessarie per l'utilizzo dell'accesso secondo le regole.

Molte strutture alberghiere, tuttavia, non gestiscono in proprio la loro rete WLAN per gli ospiti bensì aderiscono all'offerta di terzi per tale servizio. In tale contesto, l'impresa terza potrà gestire il servizio come prestatore di servizio per conto dell'hotel, oppure offrire il servizio agli ospiti dell'hotel nel proprio interesse. Tali prestatori di servizi vengono considerati in entrambi i casi come terze parti, per cui i requisiti per il coinvolgimento di terzi di cui sopra devono essere soddisfatti. Se l'hotel lascia che un fornitore di servizi offra il servizio sotto la propria diretta responsabilità, l'organizzazione del servizio conforme alla legge sulla protezione dei dati non sarà più una sua responsabilità.

i Esempio:

Un hotel svizzero lascia che la rete WLAN

venga offerta e gestita da un prestatore di servizi con sede nell'UE. Questi raccoglie i dati degli utenti a proprio nome e li elabora (anche) presso la propria sede principale nell'UE, di conseguenza dovranno essere rispettate le direttive del RGPD, ma ciò non rientra nella responsabilità dell'hotel.

Per la gestione sicura sotto il profilo legale di una rete WLAN dell'hotel, oltre alle direttive derivanti dal RGPD, dovranno naturalmente essere tenuti in considerazione anche i fondamenti giuridici locali, in particolare le direttive relative alle telecomunicazioni.

Troverete ulteriori informazioni su questa tematica sul nostro blog [mll-news.com](https://www.mll-news.com).

Avete delle domande? Siamo lieti di consigliarvi di persona.

Lukas Bühlmann, LL.M.

lukas.buehlmann@mll-legal.com
T +41 44 396 91 91

Meyerlustenberger Lachenal S.p.A

Avvocati - Attorneys at Law
Schiffbaustrasse 2 | casella postale 1765 | CH-8031 Zurigo
www.mll-legal.com | www.mll-news.com

Michaela Chvojka

michaela.chvojka@hotelleriesuisse.ch
T +41 31 370 43 46

hotelleriesuisse

Monbijoustrasse 130 | casella postale | 3001 Berna
www.hotelleriesuisse.ch