CLAVIS
CONSULTANTS LAWYERS
ACCOUNTANTS

Nicola Francione
Intellectual Property Department
n.francione@clavisroma.com
www.clavisroma.com

La privacy negli hotel: nuovo il Regolamento UE Privacy per le strutture ricettive

Il 25 maggio 2018 entra in vigore per tutti, anche per le strutture ricettive (hotel, b&b, ecc.) il **nuovo Regolamento UE n. 2016/679, in materia di Privacy**.
In linea di partenza, si osserva che:

- solo il 27% delle PMI italiane conosce i nuovi obblighi di legge derivanti dal GDPR;
- su una media di 70 aziende, solo 2 possono affermare di avere un sufficiente livello di sicurezza;
- solo una di queste due conserva i propri dati e affidi la sua gestione ad una piattaforma *cloud*.

Pertanto, il **GDPR (General Data Protection Regulation)** avrà un notevole impatto non solo dal punto di vista tecnologico, ma anche, e soprattutto, dal punto di vista organizzativo e legale.
Altri elementi di partenza sono che:

- non tutti gli alberghi sono dotati di sistema di videosorveglianza;
- non tutti gli hotel procedono ad una targetizzazione dei clienti che ospitano;
- non tutti svolgono attività di *direct marketing* di conseguenza non tutti saranno sottoposti ai medesimi obblighi.

Le modifiche introdotte dal Regolamento UE prevedono pesanti sanzioni per chi non si adegua. E' necessario che tutti gli hotel si avvalgano, in questa fase, di un professionista, un consulente, in grado di verificare e indirizzare la struttura in tutti gli adeguamenti di legge.
Inoltre, la normativa europea, direttamente applicabile in Italia, prevede che l'hotel nomini un **Responsabile per il Trattamento Dati** e, eventualmente, un **DPO** (**Data Protection Officer).** Quest'ultimo è un professionista esperto in ambito giuridico, informatico, organizzativo e in materia di *risk management*, che sia garante dell'osservazione, valutazione e gestione del trattamento dei dati, della conservazione e protezione dei dati personali secondo il GDPR: egli deve avere competenze normative, tecniche, comunicative e una profonda conoscenza dell'organizzazione del settore.
Tuttavia, non tutti gli alberghi dovranno nominare un DPO interno, ma potranno, in molti casi, anche riferirsi ad una persona esterna, ad una associazione o ad un ufficio apposito.

In questo nuovo ambito, i concetti da tenere a mente sono:

- **privacy by design:** occorre prevenire, non correggere, per cui tutte le cautele vanno adottate già in fase di progettazione e non in un secondo momento al verificarsi della mancata tutela;
- **privacy by default:** è necessario che tutte le aziende abbiano delle **impostazioni predefinite** in grado di trattare i dati dei loro clienti solo nella misura sufficiente alle finalità prefissate e rigorosamente nei tempi strettamente necessari al raggiungimento dello scopo. Affinché le impostazioni e i tempi siano rigorosamente predefiniti occorre che tutto ciò venga incluso già in fase di progettazione;
- **valutazione del rischio (DPIA):** valutazione del pericolo derivante dal trattamento, tenendo conto di i **trattamenti atti a cagionare un danno** fisico materiale o immateriale; analisi preventiva ed attenta valutazione e, eventualmente, consultazione da parte dell'Authority (Garante Privacy) per ottenere opportune indicazioni. La **DPIA *(Data Protection Impact Assessment)*** è una attività di vera ***compliance,* una procedura in grado di misurare e confermare la idoneità del trattamento** con le norme in materia di protezione dei dati personali. Si consiglia di applicarla anche ove non sia obbligatoria in quanto si tratta di un metodo estremamente utile per monitorare l'attività in essere. In realtà, è obbligatoria quanto sussistano almeno due dei criteri stabiliti dal regolamento: ad esempio, nel ramo alberghiero: 1) nel caso della videosorveglianza; 2) nel caso del trattamento dei dati sensibili;
- **Registro degli iscritti**: in esso sono descritti i trattamenti effettuati e le procedure di sicurezza adottate. Anche in questo caso, si tratta di una **"dotazione" facoltativa**, obbligatoria solo all'interno di determinate realtà (ad esempio, quando l'azienda conti un numero di dipendenti maggiori di 250). La tenuta del registro con la totalità dei trattamenti non è una mera formalità bensì una parte integrante del sistema di corretta gestione dei dati personali. Per questo al di là della dimensione dell'azienda può essere sempre consigliato dotarsi di tale registro:
- **Misure di sicurezza:** occorre che tutte le strutture adottino dei comportamenti volti a dimostrare **concretamente** la adozione di misure rivolte ad assicurare la corretta applicazione del Regolamento affidando direttamente ai titolari il compito di decidere in maniera autonoma le modalità, le garanzie e i limiti del trattamento dei loro dati;
- **Notifica delle violazioni di dati (*Data Breach)***: la notifica avviene ogniqualvolta ci sia una violazione nella procedura di sicurezza che comporta l'accidentale o illecita perdita, modifica, divulgazione o accesso dei dati personali. Ad oggi, trascorrono circa 205 giorni tra la violazione dei dati e il momento in cui l'ente o l'azienda ne viene a conoscenza. Il GDPR stabilisce che i titolari dei trattamenti saranno obbligati ad **avvisare l'Autorità di Controllo (Garante) entro 72 ore**. La violazione deve essere tale da manifestare un elevato rischio per i diritti e la libertà delle persone (inteso giuridicamente in senso fisico);
- **Informative:** tutte le informative dovranno contenere dei nuovi riferimenti. Tra le varie modifiche emerge l'introduzione del periodo di conservazione dei dati e dei criteri stabiliti per definirlo. Trascorso il periodo indicato, nasce in capo al titolare il diritto di vedersi cancellato il dato (**Diritto all'oblio)**. Il tempo di conservazione di un dato è tipicamente legato alle finalità del trattamento e il diritto all'oblio si configura come l'obbligo in capo ai titolari del trattamento non solo di procedere alla cancellazione del dato ma altresì di informare della richiesta di cancellazione gli altri titolari che trattano i dati compresi link o riproduzioni.
- **Sanzioni:** trattasi di **severo regime sanzionatorio**: le sanzioni amministrative sono molto più aspre rispetto al passato. Le ammende potranno raggiungere addirittura i 20 ML di euro ! le sanzioni amministrative entrano in gioco anche nel momento in cui non si ottempera al concetto di *Privacy by Design,* di cui sopra.

In concreto, quali sono le attività principali da compiere per rispettare il GDPR?

L'attività di ***compliance*** (rispetto della normativa) del GDPR si sostanzia in:

- richiedere agli ospiti esplicitamente il consenso alla raccolta e all'utilizzo dei dati;
- informare chiaramente i clienti su quali saranno i dati che verranno raccolti, per cosa verranno usati, da chi saranno utilizzati e per quanto tempo verranno archiviati;
- dare la possibilità alle persone di accedere ai propri dati per poterli modificare o rimuovere in qualsiasi momento;
- fornire notifiche di violazioni dei dati tramite canali specifici e all'interno di specifici intervalli di tempo;
- nel caso del salvataggio di dati digitali, assicurarsi che tali informazioni siano salvate all'interno di server sicuri e trasmessi tramite protocollo *https*;
- nominare un Responsabile della Protezione dei Dati per sorvegliare la conformità GDPR.

Qui di seguito si elencano i passaggi che deve seguire una struttura ricettiva GDPR per mettersi a norma.

1. *Mappare il flusso di dati in entrata e in uscita*

È importante conoscere quali dati vengono raccolti quotidianamente. Occorre risalire a tutte le attività con cui sono acquisite informazioni dei clienti; valutare bene quali di queste sono veramente necessarie; avere una visione precisa dei dati raccolti e delle modalità di acquisizione potrà aiutare a ridurre molto il rischio di violazioni di legge.

2. *Pulire i dati attuali raccolti*

Occorre contrassegnare i dati raccolti in archivi e cercare di ottenere un **consenso esplicito** dai diretti interessati per continuare a conservare ed utilizzare i loro dati.

3. *Formare ed aggiornare e formatr il personale interno delle strutture*

Ogni membro dello *staff* della struttura ricettiva che potenzialmente raccoglie o elabora i dati degli ospiti dovrebbe conoscere, almeno in linea generale, il GDPR e le sue implicazioni. Ancor di più, la formazione dovrebbe servire a saper gestire e utilizzare i dati degli ospiti in modo appropriato e rispettoso in ogni momento.

4. *Aggiornare le politiche sulla privacy (Privacy Policy)*

Occorre creare e/o aggiornare la *Privacy Policy* conforme a quanto richiesto dal GDPR. Qualunque sia il servizio da utilizzare, è molto importante che la *Privacy Policy* contenga i seguenti punti:

- Quali informazioni personali si raccolgono;
- Come e perché si raccolgono i dati;
- Come si usano i dati;
- Come si proteggono i dati.
- Chi sono i terzi con accesso ai dati e le loro finalità di utilizzo.
- Se e quali cookie si utilizzano.
- In che modo gli utenti possono controllare qualsiasi aspetto dei loro dati.
- Chi è il responsabile del trattamento dei dati e le loro informazioni di contatto.
- Se si usano o no i dati per prendere decisioni automatizzate.
- Qual è la base legale per il trasferimento dei dati.

5. *Aggiornare il modo in cui si raccolgono i dati*

Online: occorre documentare tutte le informazioni rilevanti relative al momento della registrazione dei dati, tra cui data/ora, indirizzo IP, metodo, ecc. Inoltre, si deve richiedere a tutte le persone che rilasceranno i loro dati di spuntare una casella per indicare che comprendono la *Privacy Policy* e che si autorizza ad attuare le varie tipologie di trattamento proposte.

Attenzione al processo di "*Lead Generation*" (generazione di una lista di possibili clienti interessati ai servizi di un hotel) su piattaforme di terzi! È infatti responsabilità del gestore dei dati accertarsi che i *lead* in arrivo da altre piattaforme abbiano autorizzato correttamente l'utilizzo dei propri dati e richiedere un'ulteriore conferma alla prima comunicazione (ad esempio: un *Lead* da campagna *Facebook* utilizzati per *newsletter marketing*).

Offline: al momento del *check-in* in hotel, sarà opportuno riferire espressamente e chiaramente ad ogni ospite quali dati si raccolgono, perché si stanno raccogliendo, per cosa saranno utilizzati e per quanto tempo saranno conservati. Naturalmente, si dovrà ottenere il consenso all'utilizzo di tali dati. Si dovrà informare i clienti che queste informazioni, su loro richiesta, potranno essere cancellati in qualsiasi momento.

6. *Prevedere una politica legata alla violazione dei dati*

Nel caso in cui si verifichi una violazione dei dati, è necessario disporre di un processo con il quale si notifica all'Auithority (Garante della Privacy), **entro 72 ore**, dell'avvenuta violazione. Inoltre, contestualmente, devono essere informati di tale violazione anche i titolari dei dati.

7. *Creare metodi per gli ospiti per modificare e rimuovere i loro dati*

Nel caso in cui un cliente richieda una copia dei propri dati, essi devono essergli forniti entro 30 giorni dalla data di tale richiesta. Il cliente può anche chiedere alla struttura che i propri dati siano cancellati. La struttura, in tal caso, dovrà procedere alla rimozione delle informazioni a meno che non ci siano accordi contrattuali differenti.

8. *Designare un DPO*

Anche se non tutte le realtà avranno l'obbligo di nominare un DPO (Data Protection Officer), sarà comunque importante avere una persona della struttura ricettiva o un operatore esterno che comprenda bene i dettagli del GDPR e che possa garantire che la struttura sia conforme a quanto richiesto dalla legge. Se nella propria struttura non si dispone di qualcuno che abbia le conoscenze o il tempo per investire in tale attività, si consiglia vivamente di affidare a un esperto esterno l'esecuzione di un controllo di conformità dei dati.

9. *Richiedere assistenza e consulenza di esperti*

Anche con un Responsabile dei Dati designato per supervisionare la conformità della struttura ricettiva, potrebbe essere comunque una buona idea richiedere un parere legale per valutare la conformità al GDPR e in particolare per effettuare una revisione delle Privacy Policy.

10. *Testare accuratamente il processo*

Va testato il processo attraverso il quale le persone forniscono i loro dati, assicurandosi che tutto funzioni come dovrebbe e che i dati, una volta acquisiti, siano utilizzati in modo appropriato; e che i titolari di tali informazioni possano modificarli, limitarne l'uso e rimuoverli in qualsiasi momento.

Fatte queste considerazioni generali ed iniziali, per il resto, si dovranno attendere i prossimi mesi, quando sarà definito meglio il cammino tracciato sul solco del Regolamento UE nonché la concreta applicazione del meccanismo sanzionatorio previsto nei confronti delle aziende "non conformi".