seisettenove

VADEMECUM GDPR

LA PRIVACY NON VA MAI IN VACANZA

Premessa

Il business alberghiero tratta dati personali per la sua natura più intima di servizio personalizzato agli individui e oltretutto, per le tendenze attuali alla disintermediazione grazie alla fidelizzazione della clientela attraverso azioni di customer relationship management e marketing automation, cade perfettamente nel paradigma della Data Economy.
I dati diventano quindi la materia prima di una nuova economia basata sulla conoscenza e sull'elaborazione delle informazioni, un potenziale motore per lo sviluppo e una fonte di nuovi business. Il GDPR, nato proprio per essere lo statuto della Data Economy, è quindi di estrema rilevanza per l'hospitality e tutti gli operatori del settore devono mettersi in regola.

Scopriamo le cose da sapere...

GLI ATTORI

Qualsiasi persona che viene a contatto con dati personali, così come qualsiasi strumento informatico e non, utilizzato per processare i dati personali di clienti, potenziali clienti, aziende, fornitori e dipendenti è soggetto al GDPR. Quindi: l'azienda alberghiera, gli strumenti aziendali, i collaboratori dell'azienda nonché i fornitori dell'hotel. Ma il ruolo che ogni strumento e/o collaboratore dell'azienda ha nel processo dei dati personali è diverso, e il GDPR identifica diverse figure di base:

- il Data Controller o Titolare del Trattamento è chi raccoglie i dati e decide come questi dati vengono utilizzati: l'azienda alberghiera è un Data Controller;
- il Data Protection Officer è una figura professionale con competenze in campo informatico, giuridico, di valutazione del rischio e di analisi di processi. Il suo compito è quello di osservare e valutare l'utilizzo dei dati personali in modo conforme al GDPR;
- il Data Processor è chi tratta i dati per conto del Data Controller, ad esempio un'OTA o un Channel Manager.

IL TRATTAMENTO DEI DATI – I PRINCIPI

20 MLN €
4% DEL FATTURATO

PRINCIPIO DI LICEITÀ, CORRETTEZZA E TRASPARENZA
I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

PRINCIPIO DI LIMITAZIONE DELLA FINALITÀ
I dati personali sono raccolti per finalità determinate, esplicite e legittime.

PRINCIPIO DI MINIMIZZAZIONE DEI DATI
I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

PRINCIPIO DI ESATTEZZA
I dati personali sono esatti e, se necessario, aggiornati.

PRINCIPIO DELLA LIMITAZIONE DELLA CONSERVAZIONE
I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

PRINCIPIO DI INTEGRITA' E RISERVATEZZA
I dati personali sono trattati in maniera da 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.

IL TRATTAMENTO LECITO DEI DATI

20 MLN €
4% DEL FATTURATO

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

INFORMATIVA SUL TRATTAMENTO DEI DATI

L'informativa sul trattamento dei dati personali è il documento con il quale il titolare del trattamento, in forma scritta o orale, informa il soggetto interessato circa le finalità e le modalità del trattamento medesimo. Indubbiamente rappresenta lo strumento atto a legittimare e a rendere trasparente la raccolta e l'utilizzo di dati personali.

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13 e 14 del Regolamento.

CONSENSO AL TRATTAMENTO DEI DATI

Il consenso è la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, trattamento del quale è stato preventivamente informato (con l'apposita informativa sulla privacy).

I DIRITTI DEGLI INTERESSATI

20 MLN €
4% DEL FATTURATO

I clienti, potenziali clienti, fornitori, contatti di aziende con cui lavoriamo normalmente nonché i collaboratori ed ex collaboratori dell'hotel acquisiscono più diritti con il GDPR.
In sintesi:

- Diritto di portabilità dei dati: una persona può trasferire i propri dati da un titolare ad un altro;
- Diritto all'oblio: i dati personali devono essere eliminati se la finalità per cui sono stati raccolti è stata raggiunta;
- Diritto all'accesso: l'interessato può richiedere di avere gratuitamente tutti i dati che lo riguardano in un formato elettronico di utilizzo comune (XML, JSON, CSV);
- Diritto alla limitazione del trattamento: l'interessato può bloccare o limitare l'utilizzo dei propri dati (ovvero: possono essere salvati, ma non possono essere utilizzati);
- Diritto all'eliminazione: l'interessato può richiedere l'eliminazione dei suoi dati quando rettifica il consenso, i dati sono stati processati in maniera illegale e/o i dati sono soggetti a eliminazione a causa di altre leggi;
- Diritto di obiezione: l'interessato può obiettare riguardo l'uso e la profilazione dei propri dati a meno che non ci sia una valida motivazione per il loro utilizzo;
- Diritti relativi alla profilazione automatica e procedure di decision making: l'interessato può negare il consenso ad eventuali procedure automatiche di profilazione che potrebbero avere un impatto dal punto di vista giuridico.

OBBLIGHI DEL TITOLARE

10 MLN €
2% DEL FATTURATO

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.
Dette misure sono riesaminate e aggiornate qualora necessario.

DATA BREACH

10 MLN €
2% DEL FATTURATO

L'art. 33 del GDPR recita che: "In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".
Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Nello specifico, l'articolo 4 p.12 del GPDR definisce la violazione dei dati personali come violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

LA DOCUMENTAZIONE – IL MODELLO ORGANIZZATIVO PRIVACY –

10 MLN €
2% DEL FATTURATO

- INFORMATIVE SUL TRATTAMENTO DEI DATI
- MODELLI PER IL CONSENSO AL TRATTAMENTO
- PROCEDURA DATA BREACH;
- PROCEDURA RICHIESTA DI ACCESSO AI DATI;
- PROCEDURA TRASFERIMENTO INTERNAZIONALE DEI DATI;
- PROCEDURA VALUTAZIONE DI IMPATTO;
- POLICY E PROCEDURE SULLA SICUREZZA DELLE INFORMAZIONI.

LA DOCUMENTAZIONE – IL MODELLO ORGANIZZATIVO PRIVACY –

10 MLN €
2% DEL FATTURATO

Come per qualsiasi altra documentazione relativa ai sistemi di gestione, valgono le seguenti regole di base:

- Deve essere completa – le cose lasciate o fatte a metà non sono mai buone;
- Deve essere in linea con il GDPR;
- Deve essere adatta alla tua azienda – assicurati che la documentazione rispecchi ciò che è stato implementato in azienda, deve essere unica. Troppe volte abbiamo visto aziende produrre una documentazione ai minimi termini, senza descrizioni dei processi o delle misure implementate: avrebbe potuto riguardare qualsiasi azienda;
- Deve essere disponibile a tutto il personale dell'azienda, seppur con diversi livelli di accesso;
- Evita duplicati – laddove possibile la documentazione dovrebbe essere strutturata in modo da evidenziare punti in comune ed evitare duplicati;
- Adotta un approccio standard – tutti i documenti devono avere lo stesso stile e layout;
- Rispetta il ciclo di vita di un documento – bozza iniziale, documento pubblicato, documento ritirato;
- Controlla i documenti e tienili aggiornati;
- Usa la posizione lavorativa al posto del nome proprio per identificare le persone.

LE FASI DELL'ADEGUAMENTO

1. PRE-ASSESSMENT

Valutazione della compliance: raccolta di tutte le informazioni sull'organizzazione aziendale, analisi e valutazione della documentazione in uso.

LE FASI DELL'ADEGUAMENTO

2. DATA - MAPPING

Una mappatura dei dati assicura all'organizzazione il controllo di come i dati si spostano o fluiscono attraverso l'organizzazione. Poiché le organizzazioni hanno bisogno di capire quali dati stanno raccogliendo, come li stanno utilizzando e con chi li condividono al fine di migliorare la protezione della privacy dei dati, la divulgazione e la conformità normativa, può anche essere un importante passo iniziale nel viaggio come importante funzione di audit.

- In questa fase si dovrà prendere totale conoscenza sulla natura dei dati strutturati o destrutturati che si archiviano in formato elettronico o su supporto cartaceo (dati anagrafici e demografici, canali di comunicazione come telefono, cellulare, email, etc.; ID nazionali come codice fiscale, passaporto, targhe, tessere sanitarie; conti bancari; identificativi digitali; riferimenti ad organizzazioni di appartenenza, social media e ulteriori dati particolari relativi alla salute) -

LE FASI DELL'ADEGUAMENTO

3. RUOLI E RESPONSABILITA'

Una mappatura dei dati assicura all'organizzazione il controllo di come i dati si spostano o fluiscono attraverso l'organizzazione. Poiché le organizzazioni hanno bisogno di capire quali dati stanno raccogliendo, come li stanno utilizzando e con chi li condividono al fine di migliorare la protezione della privacy dei dati, la divulgazione e la conformità normativa, può anche essere un importante passo iniziale nel viaggio come importante funzione di audit.

- In questa fase si dovrà prendere totale conoscenza sulla natura dei dati strutturati o destrutturati che si archiviano in formato elettronico o su supporto cartaceo (dati anagrafici e demografici, canali di comunicazione come telefono, cellulare, email, etc.; ID nazionali come codice fiscale, passaporto, targhe, tessere sanitarie; conti bancari; identificativi digitali; riferimenti ad organizzazioni di appartenenza, social media e ulteriori dati particolari relativi alla salute) -

LE FASI DELL'ADEGUAMENTO

4. INFORMAZIONE E CONSENSI

Lo scopo di questa fase è di sviluppare un modello sulla "informativa sui dati" che il titolare del trattamento deve all'interessato del trattamento, come suggerito dagli Artt.13 e 14 del Regolamento Europeo.

L'informativa da fornire deve essere la condizione base non tanto del rispetto del diritto individuale ad essere informato, quanto del dovere del titolare del trattamento di assicurare la trasparenza e correttezza dei trattamenti fin dalla fase di progettazione dei trattamenti stessi, e di essere in grado di comprovarlo in qualunque momento.

Lo sviluppo della procedura si può applicare a tutte le casistiche di categorie di interessati.

LE FASI DELL'ADEGUAMENTO

5. DEFINIZIONE DELLE POLICY

Vengono definite le policy aziendali atte a specificare le corrette modalità di esecuzione delle attività, e fornire indicazioni tecnico-organizzative.

LE FASI DELL'ADEGUAMENTO

6. REGISTRI DEI TRATTAMENTI

L'art. 30 del Regolamento (EU) n. 679/2016 prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del registro delle attività di trattamento.
E' un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del GDPR) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento (sul registro del responsabile, vedi, in particolare, il punto 6).
Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

LE FASI DELL'ADEGUAMENTO

7. RISK MANAGEMENT

Con gestione del rischio definiamo il processo di identificazione e valutazione dei rischi e la creazione di un piano che consenta di contenere o tenere sotto controllo quelli individuati e le loro conseguenze ripercuotibili su una azienda. Un rischio è una potenziale perdita o danno, ed è ascrivibile ad ambiti diversi: responsabilità legali, calamità naturali, incidenti, errori di gestione o minacce informatiche.

LE FASI DELL'ADEGUAMENTO

8. DEFINIZIONE DELLA PROCEDURA DI DATA BREACH

Prima che si verifichi un incidente di sicurezza occorre predisporre le procedure, gli strumenti e l'organizzazione per gestire l'evento fortuito al meglio.

PIANIFICAZIONE
I soggetti individuati come Soggetti Competenti devono, nel quadro del budget a loro assegnato individuare e predisporre i mezzi tecnologici ed organizzativi per Individuare, Analizzare o Rispondere alle potenziali violazioni dei dati anche coinvolgendo i fornitori.

GESTIONE DELL'EVENTO
In caso di accertamento di violazione che rientra nella definizione di Data Breach, sarà opportuno seguire i seguenti steps del processo di notificazione:

1_Acquisizione della notizia da parte dei soggetti preposti al ricevimento della violazione;
2_Analisi tecnica dell'evento;
3_Contenimento del danno;
4_Valutazione della gravità dell'evento;
5_Notifica al Garante Privacy;
6_Altre segnalazioni dovute;
7_Comunicazione agli interessati, dove necessario;
8_Inserimento dell'evento nel Registro delle Violazioni;
9_Azioni correttive specifiche e per analogia.

LE FASI DELL'ADEGUAMENTO

9. DEFINIZIONE PROCESSO DIRITTO DEGLI INTERESSATI

Il GDPR prevede che l'interessato possa esercitare diritti nei confronti del titolare del trattamento dei dati: tra questi figurano quello di accesso, di rettifica, di cancellazione. Fondamentale essere organizzati per soddisfare le richieste degli interessati entro i termini previsti dalla legge ed evitare sanzioni

LE FASI DELL'ADEGUAMENTO

10. SECURITY AWARENESS E FORMAZIONE

Gli attacchi dall'interno dell'organizzazione sono una delle maggiori minacce alla sicurezza dei dati, vuoi per azioni deliberatamente fraudolente da parte di collaboratori scontenti o infedeli, e molto più frequentemente a causa di "attacchi involontari" da parte di utenti non informati e non formati che, in modo non malevolo, rappresentano un problema per la sicurezza delle informazioni.
Visitare siti web infettati da malware, rispondere a e-mail di phishing o mantenere le proprie credenziali di accesso ai sistemi in una zona non sicura, possono causare perdite di dati molto gravi. Pertanto, tutti i collaboratori devono essere formati e informati, ripetutamente nel corso del tempo, affinché comprendano bene le responsabilità sulla sicurezza dei dati legate al proprio ruolo, le policy organizzative e come proteggere in modo adeguato le risorse a essi assegnate man mano che le potenziali minacce si evolvono.

CONSLUSIONI

CAMBIAMO PUNTO DI VISTA: IL GDPR COME OPPORTUNITA’

L’applicazione del GDPR porta con sé l’obbligo di rivedere i propri processi, investire in innovazione tecnologica e in formazione e analizzare i dati di cui si dispone sui propri clienti e, per estensione, a ragionare sulla quantità dei dati raccolti e soprattutto sulla loro qualità. Nel contesto della Data Economy la qualità delle informazioni che si possiedono diventa cruciale per il business, così come l’attenzione da parte dei media e dei consumatori verso le tematiche della sicurezza dei dati e della privacy si fa sempre più pressante.
Da questo punto di vista non può essere ignorato o sottovalutato il vantaggio competitivo che un hotel può ricavare dal data management, che è possibile solo con un sistema di gestione e controllo dei dati che comporta tutte le misure viste finora, a partire dall’avere il consenso esplicito alla profilazione e allo svolgimento di attività di marketing, al permesso di tracciare i dati nei propri sistemi informativi e così via.
È facile prevedere che i clienti daranno maggior fiducia ad un hotel che pone molta attenzione
alla privacy e alla tutela dei dati personali, a tutto vantaggio dell’immagine della struttura e, infine, dei ricavi. In definitiva, l’hotellerie può approfittare di questo cambiamento culturale per occuparsi dei clienti in maniera ancora più importante e a tutto tondo, soddisfacendo le loro aspettative con i servizi offerti e facendoli sentire ancora di più al sicuro.
E, si sa, per il piacere di sentirsi al sicuro siamo tutti disposti a spendere...

seisettenove

GDPR TASK FORCE

Piazza Carlo Magno, 21
00162 Roma

Tel: 06 99312465 | Email: info@seisettenove.it

www.seisettenove.com