

DECALOGO PRIVACY PER LE STRUTTURE ALBERGHIERE

INDICE

INTRODUZIONE

1 – INFORMATIVA

2 – CONSENSO

3 – SCHEDE DI DICHIARAZIONE

4 – BOOKING ON-LINE

5 – INTERNET POINT / SERVIZI DI CONNESSIONE INTERNET

6 – SISTEMI DI VIDEOSORVEGLIANZA

7 – WEB CAM

8 – LETTERE DI NOMINA DI RESPONSABILI / INCARICATI / ADDETTI

9 – MISURE DI SICUREZZA

10 – DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

CONCLUSIONI

Copyright 2006 – Dr. Eric Falzone

Via A. Gloria 21 – 35030 Rubano (PD) – Tel. 348-6916273 – Fax 049-631246 – E-mail: eric.falzone@eucs.it

Tutti i diritti sono riservati.

La riproduzione, modifica e utilizzo di qualsiasi parte del presente documento è consentita solo previa autorizzazione dell'Autore.

E' comunque escluso ogni utilizzo del contenuto del presente documento per la redazione di ulteriori saggi, testi o pubblicazioni.

Fonti: *Decreto legislativo 30 giugno 2003, n. 196 - Newsletter del Garante – D.L. 144/05 - “Legge Pisanu’ - Testo Unico delle Leggi di Pubblica Sicurezza (T.U.L.P.S.) - Provvedimento Generale per Videosorveglianza emanato dall’Autorità Garante per la Protezione dei Dati Personali il 29 Aprile 2004.*

INTRODUZIONE

Tra centinaia di turisti e ospiti che ininterrottamente si avvicendano ed i classici problemi relativi alla prenotazione, gestione ed assistenza della clientela, ogni singola struttura alberghiera si trova giornalmente a dover acquisire un ingente mole di dati personali che, se non trattati correttamente, possono rivelarsi "potenzialmente pericolosi" sotto il profilo della disciplina Privacy.

Ecco quindi un decalogo che ogni albergatore dovrebbe sempre tenere a portata di mano al fine di verificare la corretta applicazione della disciplina prevista dal Codice Privacy (D.Lgs 196/03) presso la propria struttura.

1 - INFORMATIVA

Ogni struttura alberghiera deve predisporre un'informativa chiara e comprensibile (che contenga almeno i requisiti minimi previsti dall'art 13 del D.Lgs 196/03) da consegnare al cliente al momento della raccolta e registrazione dei dati personali e nella quale venga adeguatamente spiegato l'uso che verrà fatto di tali dati (ad esempio per compiere operazioni di prenotazione o per assolvere agli obblighi previsti dal T.U.L.P.S.)

Qualora si volessero raccogliere dati per finalità di marketing (ad es. questionari di gradimento), per invio di comunicazioni commerciali (ad es. Newsletter), per operazioni di fidelizzazione (ad es: Carta Fedeltà) o per la definizione dei profili di consumo della clientela (ad es: classificazione di gusti, abitudini, consumi...) è consigliabile preparare un'ulteriore informativa nella quale spiegare dettagliatamente le finalità e modalità di trattamento dei dati raccolti a tale scopo.

2 - CONSENSO

Oltre all'informativa è necessario poi predisporre un modulo per l'acquisizione del consenso da far sottoscrivere al cliente, distinguendo opzioni diverse per l'autorizzazione al trattamento di dati personali comuni, l'autorizzazione al trattamento di dati sensibili/giudiziari e l'autorizzazione al trattamento di dati per finalità di marketing, comunicazione commerciale o profilazione delle scelte di consumo.

Per quanto riguarda il consenso da parte del cliente, questo non è richiesto nel caso si trattino dati personali comuni esclusivamente al fine di adempiere ad obblighi di legge/regolamento (ad esempio, per assolvere ad obblighi contabili e tributari o previsti dal T.U.L.P.S.) o per compiere operazioni di trattamento in fase contrattuale o precontrattuale.

Il consenso scritto invece, è sempre obbligatorio qualora si raccolgano dati sensibili e/o giudiziari o si intendano compiere operazioni di marketing, profilazione od invio di comunicazioni commerciali.

3 - SCHEDE DI DICHIARAZIONE

In tema di obblighi normativi previsti dal T.U.L.P.S., la disciplina privacy prevede che le "schede di dichiarazione" in cui vengono riportati i dati personali sottoscritti dal cliente, siano trasmesse in questura entro ventiquattro ore dall'arrivo in albergo e consegnate alle autorità di P.S. in maniera "diretta" senza il tramite di altri enti o soggetti. Una volta assolto l'obbligo di comunicare i dati alle autorità di pubblica sicurezza tramite computer o su carta, le schede non devono essere conservate, ma distrutte. In ogni caso i dati acquisiti con le schede di dichiarazione non potranno mai essere conservati se non per fini fiscali e contabili e nella misura a ciò strettamente necessaria.

4 – BOOKING ON-LINE

Nel caso di raccolta di dati personali tramite internet o posta elettronica, al fine di compiere operazioni di prenotazione o per adempiere a specifiche richieste del cliente, è consigliabile la pubblicazione di un'adeguata informativa on-line e l'acquisizione preventiva del consenso via web secondo le modalità specificate ai punti 1 e 2.

5 – INTERNET POINT / SERVIZI DI CONNESSIONE INTERNET

Qualora si offra alla clientela un servizio di navigazione o connessione internet si è soggetti alla disciplina della “*Legge Pisanu*” (D.L. 144/05).

In particolare vi è l'obbligo di richiedere al questore una licenza per la messa a disposizione alla clientela od al pubblico di apparecchi terminali utilizzabili per comunicazioni telematiche.

Inoltre si devono acquisire e conservare i dati identificativi e del traffico dei clienti che hanno utilizzato servizi di connessione alle reti telefoniche e telematiche.

L'identificazione può avvenire anche contestualmente a quella richiesta a norma dell'art. 109 del T.U.L.P.S.

Le informazioni da conservare sono: i dati anagrafici dell'utilizzatore, una copia del documento di identità ed i “log file” che contengono i dati del traffico.

6 – SISTEMI DI VIDEOSORVEGLIANZA

Se ci si avvale di sistemi di videosorveglianza per la protezione della struttura alberghiera, bisogna verificare che siano adottate tutte le prescrizioni previste dal Codice Privacy e dal “*Provvedimento Generale per Videosorveglianza emanato dall'Autorità Garante per la Protezione dei Dati Personali il 29 Aprile 2004*”.

In particolare vi è l'obbligo di prevedere che nelle vicinanze di ogni telecamera sia affisso cartello con un'informativa semplificata; bisognerà poi predisporre una completa informativa da esporre all'interno dell'albergo e redigere una “*Relazione sul Sistema di Videosorveglianza Aziendale*” nella quale siano spiegate e documentate le finalità, le modalità e le scelte aziendali in materia di videosorveglianza.

Ulteriori adempimenti sono l'adozione delle misure minime di sicurezza e la predisposizione di lettere di nomina per Responsabili ed Incaricati al trattamento ed addetti alla gestione e manutenzione dell'impianto.

La conservazione delle immagini sarà sempre limitato a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione.

7 – WEB CAM

Qualora si utilizzino web cam per fini promozionali, turistici o pubblicitari è sempre necessario provvedere all'affissione di un cartello di avviso nelle immediate vicinanze dell'area di ripresa e di una completa informativa nella quale vengano illustrate modalità e finalità della raccolta delle immagini.

Le telecamere installate poi devono avere una bassa risoluzione, essere fisse e prive di zoom e posizionate lontano dalla zona di ripresa.

In qualunque caso è severamente vietato rilevare immagini che possano rendere identificabili i soggetti ripresi.

8 – LETTERE DI NOMINA DI RESPONSABILI / INCARICATI / ADDETTI

Per ogni struttura alberghiera è consigliabile definire almeno un "Responsabile Privacy Interno", da nominare con lettera scritta, che si occupi della gestione delle problematiche inerenti il trattamento di dati personali.

Tutto il personale che ha accesso ai dati poi deve essere "incaricato" per iscritto con una lettera di nomina, nella quale devono essere definite dettagliatamente istruzioni operative e ambito di trattamento ad ognuno di essi consentito.

Qualora ci si avvalga di aziende esterne per il trattamento di dati personali bisognerà provvedere a nominarle quali "Responsabili Esterni"; qualora invece ci si faccia supportare tecnicamente da aziende informatiche bisognerà incaricarle come "Addetti Esterni alla Manutenzione del Sistema Informatico".

9 – MISURE DI SICUREZZA

Per il trattamento di dati personali bisognerà sempre rispettare quanto previsto dal Codice Privacy in tema di misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

In particolare si dovrà verificare la completa applicazione di quanto previsto dagli art. 33 e 34 del D.Lgs 196/03 e di quanto disciplinato nell'Allegato B).

10 – DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

Per quanti trattino dati personali sensibili o giudiziari con strumenti elettronici è obbligatoria la redazione del "Documento Programmatico sulla Sicurezza (DPS)" secondo le modalità previste dalla regola 19 dell'Allegato B).

Anche per quanti non fossero soggetti al DPS, risulta comunque sempre caldamente consigliabile la stesura di una "Relazione Privacy", in cui definire le finalità e modalità del trattamento dei dati personali raccolti e le misure di sicurezza adottate.

CONCLUSIONI

Si rammenta che la mancata applicazione della normativa vigente in materia di Privacy, espone al rischio di pesanti sanzioni amministrative (art. 161, 162, 163 e 164 – D.Lgs 196/03) e penali (art. 167, 168, 169, 170 e 171 - D.Lgs 196/03).

In particolare per omessa o inidonea informativa si potrà essere soggetti ad una sanzione da €. 3.000,00 a €. 18.000,00; per trattamento illecito di dati ad una reclusione da 6 mesi a 3 anni; per mancata adozione delle misure di sicurezza all'arresto sino a 2 anni o ad un'ammenda da €. 10.000,00 a €. 50.000,00.