La protezione dei dati personali nella gestione delle imprese ricettive

terza edizione

Federica Bonafaccia

in collaborazione con

FORMAT

FEDERALBERGHI

LA PROTEZIONE DEI DATI PERSONALI
NELLA GESTIONE DELLE IMPRESE RICETTIVE

la privacy nell'ospitalità

terza edizione

La protezione dei dati personali nella gestione delle imprese ricettive

(la privacy nell'ospitalità)

di Federica Bonafaccia

EDIZIONI ISTA

Istituto Internazionale di Studi

e Documentazione Turistico Alberghiera

"Giovanni Colombo"

00187 Roma – via Toscana 1

INDICE

IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(Decreto Legislativo 196/2003)

la struttura del Codice

Dal 1° gennaio 2004 è in vigore il “Codice in materia di protezione dei dati personali”, approvato con il Decreto Legislativo 30 giugno 2003, n. 196, e conseguentemente da quella data risulta abrogata la legge 675/1996 e tutti i regolamenti ad essa collegati.

Il Codice è strutturato in tre parti:

- Parte I (artt. 1-45) contenente le disposizioni generali;
- Parte II (artt. 46-140) contenente le disposizioni inerenti a specifici settori (Ambito giudiziario, Forze di Polizia, Difesa e sicurezza dello Stato, Ambito pubblico, Ambito sanitario, Istruzione, Trattamento per scopi storici, statistici o scientifici, Lavoro e previdenza sociale, Sistema bancario, finanziario ed assicurativo, Comunicazioni elettroniche, Libere professioni e investigazione privata, Giornalismo ed espressione letteraria ed artistica, Marketing diretto);
- Parte III (artt. 141-186) concernente la tutela dell’interessato, le sanzioni, le disposizioni modificative, abrogative, transitorie e finali.

Seguono una serie di allegati (codici di deontologia, disciplinare tecnico in materia di misure minime di sicurezza ed elenco dei trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia).

la finalità della normativa

La normativa sulla privacy ha recepito nel nostro ordinamento una direttiva comunitaria del 1995[1], ma ha avuto anche e soprattutto il merito di introdurre nel diritto positivo del nostro paese il principio secondo il quale la riservatezza delle persone costituisce un diritto assoluto ed inviolabile, meritevole di tutela attraverso la comminazione di sanzioni civili, penali ed amministrative.

La normativa si pone pertanto come obiettivo la tutela di due diversi beni:

- il diritto alla riservatezza delle persone, e cioè la protezione di quei dati attinenti alla sfera intima della persona, la cui diffusione, pur non costituendo vera e propria offesa all'onore o al decoro, non è comunque di utilità pubblica o sociale;
- il diritto all'identità personale, al fine di evitare che ad una determinata persona vengano attribuiti atti o comportamenti che, seppure non lesivi della dignità, dell'onore o del decoro, non siano corrispondenti al vero.

Rispetto alla direttiva comunitaria, la normativa italiana ha inizialmente voluto estendere la tutela anche ai dati personali delle persone giuridiche, degli enti e delle associazioni, oltre che delle persone fisiche, suscitando perplessità e dubbi tra gli stessi parlamentari. Ai dati delle persone non fisiche veniva comunque attribuita nel concreto una tutela affievolita, sicuramente non paragonabile a quella assicurata ai dati delle persone fisiche.

Nel 2011, con il Decreto "Salva Italia"[2], sono stati eliminati dal campo di applicazione del Codice della privacy i trattamenti di dati che riguardano le persone giuridiche, gli enti e le associazioni. La tutela del Codice della privacy rimane pertanto assicurata solo per i trattamenti che riguardano le persone fisiche.

[1] Direttiva comunitaria 95/46/CE del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; pubblicata in Gazzetta Ufficiale delle Comunità europee L 281 del 23 novembre 1995.

[2] Decreto Legge 6 dicembre 2011 n. 201, articolo 40.

le definizioni

Per comprendere la normativa ed il suo campo di applicazione, è indispensabile analizzare alcune definizioni tra quelle riportate nell'articolo 4 del Codice:

- *"Trattamento":* qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.
- *"Dato personale"*: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
- *"Dati sensibili"*: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
- "*Dati giudiziari*": i dati personali idonei a rivelare alcuni tipi di provvedimenti giudiziari, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato;
- *"Titolare"*: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- *"Responsabile":* la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
- *"Incaricati":* le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- *"Interessato":* la persona fisica cui si riferiscono i dati personali.
- *"Comunicazione":* il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- "*Diffusione":* il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- "*Dato anonimo*": il dato che in origine o a seguito di trattamento non può essere associato ad un interessato identificato o identificabile.
- *"Blocco":* la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

- *“Banca dati”:* qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
- *“Garante”:* organo collegiale costituito da quattro membri che opera in piena autonomia e indipendenza per verificare il rispetto delle disposizioni vigenti sui trattamenti dei dati per la tutela delle persone.

Il Codice definisce inoltre:

- *"misure minime"*, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto;
- *"strumenti elettronici"*, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- *"autenticazione informatica"*, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- *"credenziali di autenticazione"*, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
- *"parola chiave"*, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- *"profilo di autorizzazione"*, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- *"sistema di autorizzazione"*, l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

il campo di applicazione

Secondo quanto stabilisce l'articolo 5, le disposizioni del Codice si applicano al trattamento di dati personali da chiunque effettuato nel territorio dello Stato. Nel campo di applicazione della normativa sono ricompresi anche i trattamenti di dati personali effettuati da chi si sia stabilito nel territorio di un paese extra U.E. ma impieghi, per il trattamento, mezzi, anche non elettronici, situati nel territorio italiano, escluso il caso di utilizzo solo a fini di transito nel territorio dell'U.E. In tali casi il titolare deve designare un proprio rappresentante stabilito nel territorio italiano.

Come abbiamo visto nella definizione di "trattamento", la legge non limita le sue prescrizioni al solo momento della registrazione informatica dei dati personali, ma assicura ampia tutela ai dati personali durante ogni operazione, sia che avvenga con l'ausilio di mezzi elettronici, sia che avvenga senza tale ausilio.

Unico limite rispetto a tale estensione riguarda il trattamento di dati personali effettuato da persone fisiche. Tale trattamento, infatti, se effettuato per fini esclusivamente personali, non è soggetto all'applicazione della legge, sempre che i dati non siano destinati ad una comunicazione sistematica o alla diffusione, e fatto salvo l'obbligo di adottare misure minime di sicurezza e di risarcire il danno eventualmente causato.

Pertanto, chi tratta dati nominativi per fini esclusivamente personali (ad esempio, la rubrica telefonica con i contatti non professionali) non è tenuto agli adempimenti previsti dal Codice, ma è però tenuto a custodire tali dati adottando tutte le misure di sicurezza idonee a prevenire i rischi della loro distruzione o perdita o di accesso abusivo o di utilizzazione abusiva. In mancanza di tali cautele, è possibile l'attribuzione della responsabilità civile e la condanna al risarcimento dei danni.

il Garante

Il “Garante per la protezione dei dati personali” (articolo 153) è un organo collegiale, costituito da quattro membri, nominati due dalla Camera e due dal Senato.

Attualmente è così composto: Antonello Soro *(Presidente)*, Augusta Iannini *(vice Presidente)*, Giovanna Bianchi Clerici, Licia Califano. Il Segretario Generale è il Dott. Giuseppe Busia.

L’Autorità Garante per la protezione dei dati personali è stata istituita al fine di tenere un registro generale dei trattamenti e di controllare se i trattamenti siano effettuati nel rispetto della relativa disciplina.

Alle dipendenze del Garante è posto uno specifico Ufficio la cui organizzazione e funzionamento è disciplinata dagli articoli 155 e seguenti del Codice.

Oltre a stabilire norme sull'organizzazione interna dell'Ufficio dell’Autorità Garante, il Codice regolamenta le modalità per l'esercizio e la tutela dei diritti dei cittadini in materia di trattamento dei dati personali, nonché per l’effettuazione degli adempimenti previsti dal Codice a carico dei titolari di banche dati (richieste di autorizzazioni, notificazioni ecc.).

Il Codice regolamenta inoltre le modalità per l’attivazione e la definizione del procedimento amministrativo davanti all'Autorità Garante. E’ infatti prevista la possibilità di adire l'Autorità Garante per la protezione dei dati personali in caso di lesione di diritti in materia di privacy, in alternativa al ricorso all'Autorità giudiziaria ordinaria.

Il Codice evidenzia infine gli elementi distintivi tra la semplice segnalazione ed il reclamo, che non richiedono particolari formalità per la loro presentazione e che sono comunque esaminati dal Garante, ed il vero e proprio ricorso.

le forme di tutela

L'interessato può rivolgersi al Garante:

- mediante reclamo, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
- mediante segnalazione, se non è possibile presentare un reclamo, al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
- mediante ricorso.

Il **reclamo** (artt. 142 e 143) deve contenere un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare, del responsabile, ove conosciuto, e di cui colui che presenta l'istanza.

Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano anche ai sensi dell'articolo 9, comma 2, del Codice ed è presentato al Garante senza particolari formalità. Al reclamo deve essere allegata la documentazione utile ai fini della sua valutazione.

Se ne sussistono i presupposti, il Garante può adottare i seguenti provvedimenti, anche prima della definizione del procedimento:

- prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;
- dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto, oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;
- può vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettività.

I provvedimenti sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.

La **segnalazione** non richiede particolari formalità di presentazione. L'interessato si rivolge al Garante mediante la segnalazione quando non è possibile presentare un reclamo circostanziato, ma ritiene comunque di sollecitare un controllo da parte del Garante sulla corretta applicazione della disciplina in materia di trattamento di dati personali.

Il Garante può adottare i provvedimenti di cui sopra anche a seguito di segnalazioni.

Il **ricorso** ha invece carattere formale. La presentazione del ricorso al Garante rende improponibile la stessa domanda dinanzi all'Autorità Giudiziaria Ordinaria, che comunque potrà essere successivamente adita in opposizione. Risulta in questo modo recepito il principio di alternatività tra l'esercizio dell'azione giurisdizionale e la presentazione del ricorso davanti al Garante.

Il ricorso al Garante può essere proposto solo dopo che è stato effettuato l'interpello preventivo. L'articolo 146 del Codice prescrive infatti che, fatti salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso può

essere presentato solo dopo che l’interessato ha interpellato sulla questione il titolare o il responsabile del trattamento ai sensi dell'articolo 8, comma 1.

In tal caso, il riscontro alla richiesta da parte del titolare o del responsabile deve essere fornito all’interessato entro quindici giorni dal suo ricevimento. Se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima.

Decorsi tali termini, ovvero nel caso in cui è stato opposto alla richiesta un diniego anche parziale, l’interessato potrà presentare ricorso ai sensi dell’articolo 147 del Codice.

Il procedimento si attiva quindi su impulso di parte e si ispira allo schema processuale del patteggiamento: è infatti prevista la preliminare richiesta da parte del Garante al titolare o al responsabile del trattamento di aderire spontaneamente alla richiesta di tutela avanzata dal ricorrente.

L'adesione spontanea, se da una parte determina una sorta di non luogo a procedere del giudizio, dall'altra prevede la condanna alle spese, sempre se richieste, e che l'Autorità liquiderà in misura forfetaria.

Contestualmente alla comunicazione del ricorso ed alla richiesta di adesione spontanea, il Garante indica il termine in cui il titolare, il responsabile del trattamento nonché l'interessato possono presentare memorie e documenti e la data di eventuale audizione in contraddittorio anche mediante videoconferenza.

Le parti possono stare in giudizio personalmente e non è necessaria un'assistenza legale. Il provvedimento, anche provvisorio o di rigetto, adottato dal Garante è comunicato alle parti entro tre giorni presso il domicilio eletto o, in mancanza, presso quello indicato nel ricorso o nelle memorie.

Se vi è stata previa richiesta di taluna delle parti, il provvedimento che definisce il procedimento determina in misura forfetaria l'ammontare delle spese e dei diritti inerenti al ricorso posti a carico, anche in parte, del soccombente.

I provvedimenti, infine, vengono pubblicati sul Bollettino del Garante.

I provvedimenti del Garante sono ricorribili mediante proposizione di opposizione dinanzi al Tribunale del luogo di residenza del titolare del trattamento. Tale impugnativa, che comunque non sospende il provvedimento, deve essere esercitata entro trenta giorni dalla data di comunicazione del provvedimento dell'Autorità.

i diritti dell’interessato

L’articolo 7 del Codice attribuisce all’interessato una serie di diritti, tra cui:

- il diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano;
- il diritto di ottenere informazioni sull’origine dei dati personali, sulle finalità e modalità del trattamento, sulla logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, sull’identità del titolare e degli eventuali responsabili, sui soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza;
- il diritto di ottenere l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge.

L'interessato ha diritto di opporsi, in tutto o in parte:

- per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il controllo dell'interessato sui dati che lo riguardano è pertanto un controllo finalizzato in primo luogo a constatare l'esattezza del dato stesso, ed in secondo luogo a verificare la correttezza nell'utilizzo del dato trattato. Inoltre, tale controllo può estendersi sia al soggetto che è in possesso di quel dato sia all'attività del medesimo.

Si tratta, in altri termini, di un potere da far valere, che è giustificato non solo dall'interesse primario che il dato trattato sia corretto, ma anche dalla possibilità che ha l'interessato di difendersi di fronte ai possibili abusi conseguenti ad un illecito trattamento del dato.

L’interessato ha anche diritto di accedere gratuitamente al Registro detenuto presso il Garante, dove sono inseriti i trattamenti previsti dall’articolo 37 del Codice, suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, soggetti all’obbligo di notifica.

L’accesso può anche essere svolto mediante delega o procura ad altre persone fisiche o ad associazioni, conferite necessariamente per iscritto. In tal modo l’interessato dispone di uno strumento in più, nel caso in cui non abbia la capacità o competenza di esprimere da solo una effettiva difesa.

L'accesso è finalizzato, peraltro, oltre che a consentire una verifica dei dati trattati, anche ad ottenere una serie di provvedimenti che pongano rimedio all'eventuale inesattezza dei medesimi.

Accanto alla cancellazione o trasformazione in forma anonima dei dati in contrasto con la legge o non inerenti le finalità di trattamento, viene concessa un'ulteriore possibilità: ottenere l'aggiornamento, la rettifica o l'integrazione del dato.

Il Legislatore attribuisce infine all’interessato la possibilità di opposizione al trattamento dei dati, giustificata da motivi legittimi.

Opposizione che la legge prevede esplicitamente con riferimento ai casi di trattamento dei dati personali inerenti ad informazioni commerciali ed al ricorrente invio di materiale pubblicitario o per il compimento di ricerche di mercato.

La risposta del titolare, o del responsabile, alle richieste conseguenti all'accesso deve essere formulata "senza ritardo", cioè con immediatezza e sollecitudine.

l’informativa

L’articolo 13 del Codice prevede che, all’atto della raccolta di dati personali, l’interessato, o la persona presso la quale i dati sono raccolti, debba ricevere una serie di informazioni, oralmente o per iscritto, tra cui:

- informazioni sui suoi diritti, nonché sulle finalità e modalità del trattamento;
- informazioni sulla natura obbligatoria o facoltativa del conferimento dei dati, e sulle conseguenze di un rifiuto di rispondere;
- informazioni sui soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza;
- informazioni sulle generalità del titolare e del responsabile.

L’informativa non è dovuta nel caso di ricezione di curricula spontaneamente trasmessi dagli interessati al fine dell’eventuale instaurazione di un rapporto di lavoro. Nel caso di contatto successivo, il titolare dovrà però fornire una breve informazione sul trattamento, anche orale (art. 13, comma 5 bis).

Il diritto ad una corretta ed esauriente informativa assume una particolare importanza per il controllo della correttezza del trattamento dei dati personali e per valutare il comportamento tenuto dal titolare della banca dati.

Nel caso di dati raccolti presso terzi, il Codice prevede che l’interessato debba ricevere l’informativa all’atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

Non è invece necessario informare l’interessato, sempre e solamente nel caso di dati raccolti presso terzi, quando:

- i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- i dati sono trattati ai fini dello svolgimento delle “investigazioni difensive”, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
- l'informativa all'interessato comporti un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

Tali circostanze, previste nell’ultimo punto, sono valutate in concreto dal Garante caso per caso, con particolare riguardo alla speciale natura delle finalità perseguite o dei dati trattati, alle complesse modalità di realizzazione dell’adempimento, all’ingente numero degli interessati, alle attività necessarie per rintracciarli, alla data di raccolta delle informazioni o alla particolare onerosità dei costi da sostenere.

Il Garante potrà autorizzare anche, in circostanze particolari, modalità di informazione sostitutive, attraverso, ad esempio, avvisi pubblici o per pubblici proclami o annunci periodici specie sulla stampa nazionale o locale anche specializzata. Sarà quindi possibile per alcuni titolari del trattamento perseguire comunque, in misura ragionevole, le finalità proprie dell’informativa.

Tali eccezioni, ribadiamo, non riguardano però i casi in cui i dati siano forniti direttamente dall'interessato o, a prescindere dalle modalità della loro raccolta, possano essere trattati solo in presenza del consenso. Infatti, come vedremo in seguito, il consenso può ritenersi prestato validamente solo se l'interessato ha ricevuto una previa ed idonea informativa. In entrambi i casi, pertanto, il Codice non prevede un esonero, né attribuisce al Garante la possibilità di sottrarre alcune notizie dall'obbligo di informativa.

Abbiamo detto che l'informativa può anche essere data oralmente, ma in tal caso diventa difficile provare l'avvenuto adempimento in caso di contestazioni. Per questo motivo, qualora si debbano effettuare trattamenti per i quali è necessario il consenso dell'interessato, è opportuno inserire l'informativa scritta all'interno del modulo di consenso, così da poter disporre di certezza probatoria nel caso d'eventuali contestazioni .

Il Garante ha comunque in più occasioni chiesto maggiore trasparenza, semplicità e non contraddittorietà del messaggio che il titolare del trattamento, ai sensi dell'articolo 13 del Codice, è tenuto a rivolgere all'interessato.

L'obiettivo della legge è infatti la conoscenza effettiva da parte dell'interessato dei caratteri del trattamento e dei diritti connessi, privilegiando la sostanza piuttosto che la forma.

le sanzioni - L'articolo 161 del Codice sanziona l'omessa o inidonea informativa con la sanzione amministrativa da 6.000 a 36.000 Euro.

Nei casi di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi sopra indicati sono applicati in misura pari a due quinti.

il consenso

L’articolo 23 del Codice legittima il trattamento di dati personali solo se è stato acquisito il consenso espresso dell'interessato. Il consenso può riguardare l’intero trattamento o una o più operazioni dello stesso.

Il consenso è valido solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se è stata fornita una adeguata informativa (consenso informato).

Come vedremo in seguito, il consenso deve essere necessariamente manifestato in forma scritta quando il trattamento riguarda dati sensibili.

L’articolo 24 del Codice consente il trattamento anche senza consenso in alcuni casi, tra i quali:

- quando il trattamento è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- quando il trattamento è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- quando il trattamento riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
- quando il trattamento riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo;
- nei casi individuati dal Garante, quando il trattamento, esclusa la diffusione, è effettuato per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell’interessato;
- quando il trattamento, con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
- quando il trattamento riguarda dati contenuti nei curricula spontaneamente trasmessi dagli interessati ai fini dell’eventuale instaurazione di un rapporto di lavoro.

L’articolo 25 del Codice stabilisce infine che i dati personali non possono comunque essere comunicati o diffusi:

- in caso di divieto disposto dal Garante o dall'autorità giudiziaria;
- nel caso in cui ne è stata ordinata la cancellazione;
- quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e), e cioè il tempo necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
- per finalità diverse da quelle indicate nella notificazione del trattamento al Garante, ove prescritta.

E' evidente, quindi, che per le attività di comunicazione e diffusione dei dati personali il regime previsto dal Codice è più rigoroso rispetto a quanto previsto per il generico trattamento. Presumendo infatti che la comunicazione e la diffusione dei dati personali costituiscano le operazioni del trattamento per loro natura maggiormente lesive della riservatezza, la normativa prevede casi più limitati di esclusione della necessità del consenso.

Secondo il Garante[3], inoltre, sulla base dei principi generali dell'ordinamento giuridico e delle regole dettate a livello comunitario il consenso può essere ritenuto effettivamente libero solo se è prestato al riparo da qualsiasi pressione e non è condizionato dall'accettazione di clausole che determinino uno squilibrio nelle posizioni delle parti del contratto.

Pertanto, la richiesta di un consenso generale ed incondizionato, proveniente da un soggetto in posizione contrattuale più forte rispetto al destinatario dell'informativa, si risolve in una violazione della libertà contrattuale di quest'ultimo. Ciò è esattamente quanto avverrebbe nel caso di un consenso generalizzato e fondato su informazioni generiche o insufficienti, accompagnate dall'esplicita previsione di una possibile rottura dei rapporti contrattuali. In tal modo verrebbero infatti negati proprio i diritti definiti dalla normativa come "fondamentali".

La normativa richiede che il consenso venga prestato “in forma specifica”, e cioè venga riferito ad un preciso trattamento effettuato da un ben individuato soggetto.

In conseguenza, quando il soggetto titolare di trattamento intende acquisire il consenso dell'interessato anche per l'utilizzazione dei suoi dati da parte di altri soggetti, questi ultimi devono essere indicati puntualmente.

Inoltre, poiché il consenso è valido solo se è fornita l’informativa, l'informativa stessa deve riguardare anche le eventuali attività svolte da terzi, che dovranno essere indicati in modo preciso ed esaustivo, al fine di consentire all'interessato di avere piena consapevolezza dei soggetti in favore dei quali il consenso è riferito.

le sanzioni - L’articolo 167 del Codice stabilisce che, salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, proceda al trattamento di dati personali in violazione alle prescrizioni relative al consenso di cui all’articolo 23 del Codice, è punito, se dal fatto deriva nocumento, con la reclusione da 6 a 18 mesi o, se il fatto consiste nella comunicazione o diffusione di tali dati, con la reclusione da 6 a 24 mesi.

Inoltre, salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, proceda alla comunicazione o diffusione dei dati personali nei casi vietati dall’articolo 25 è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

---

[3] Decisione del Garante per la protezione dei dati personali del 28.5.1997, relativa ai moduli di informativa adottati dalla Banca Nazionale del Lavoro - doc. web n. 40425

la notificazione al Garante

Il titolare che intenda procedere ad un trattamento di dati personali è tenuto a darne notificazione al Garante solo se il trattamento, per le modalità o la natura dei dati trattati, sia suscettibile di recare pregiudizio ai diritti ed alle libertà degli interessati.

L'articolo 37 del Codice elenca i trattamenti sottoposti all'obbligo di notificazione:

- dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Il Garante ha inoltre provveduto con apposita Deliberazione[4] a chiarire l'ambito di applicazione dell'articolo 37, individuando più specificamente i trattamenti di dati personali (raccolta, uso, conservazione ecc.) non soggetti all'obbligo di notificazione.

Il provvedimento del Garante contiene in effetti ulteriori semplificazioni, rispetto a quanto genericamente previsto dall'articolo 37 del Codice, che interessano soprattutto società, enti locali, operatori sanitari (in particolare medici di medicina generale e pediatri), liberi professionisti, datori di lavoro e gestori di impianti di videosorveglianza.

Sulla base delle semplificazioni introdotte, risulta chiaro che non è previsto l'obbligo di effettuare la notificazione al Garante per i trattamenti normalmente effettuati dalle imprese ricettive, quali ad esempio:

- trattamento dei dati dei clienti che effettuano una prenotazione alberghiera;
- trattamento dei dati dei clienti registrati ai fini della notifica di polizia;
- trattamento dei dati dei clienti durante il soggiorno;
- trattamento dei dati dei clienti effettuato a fini fiscali;

[4] Deliberazione n. 1 del 31 marzo 2004 dell'Autorità Garante per la protezione dei dati personali, pubblicata nella Gazzetta Ufficiale n. 81 del 6.4.2004.

- trattamento dei dati dei clienti effettuato per l'invio di materiale pubblicitario o per iniziative promozionali;
- trattamento dei dati dei lavoratori;
- trattamento dei dati dei fornitori;
- trattamento dei dati delle agenzie di viaggi o tour operator.

Con una ulteriore nota sull'argomento[5], per quanto riguarda la localizzazione di persone o oggetti, il Garante ha provveduto inoltre a chiarire che non devono essere notificati:

- i trattamenti che consentono soltanto una rilevazione non continuativa del passaggio o della presenza di persone o oggetti quali i badge utilizzati per la registrazione di ingressi o uscite sul luogo di lavoro;
- la videosorveglianza anche con impianti a circuito chiuso a meno che il titolare non possa rilevare anche le diverse ubicazioni o gli spostamenti di una persona in determinati luoghi o aree sul territorio;
- la lettura di carte elettroniche per fornire beni o prestare servizi (es. carte di pagamento, di credito o di fidelizzazione).
- i trattamenti effettuati al solo fine di:
  - ⇒ fornire all'interessato beni, prestazioni o servizi senza alcuna profilazione degli interessati
  - ⇒ verificare l'identità o il profilo di autorizzazione di utenti o incaricati
  - ⇒ registrare gli accessi ad un sito web (solo se memorizzati per il tempo strettamente necessario a fini di sicurezza o di elaborazione statistica in forma anonima)
- i trattamenti effettuati dai CAAF per adempimenti fiscali o contabili (es. redazione bilanci)
- i trattamenti relativi alla fornitura di beni, prestazioni di servizi o adempimenti contabili o fiscali.

Sono invece soggetti all'obbligo di notificazione i trattamenti di immagini o suoni (cioè la videosorveglianza) che, anche se registrati temporaneamente, siano inseriti in apposite banche di dati elettroniche relative a comportamenti illeciti o fraudolenti.

La notificazione, ove necessaria, deve essere effettuata preventivamente ed una sola volta, a prescindere dal numero delle operazioni da svolgere nonché dalla durata del trattamento, e può riguardare uno o più trattamenti con finalità correlate.

La notificazione è possibile solo per via telematica e con sottoscrizione con firma digitale (www.garanteprivacy.it).

le sanzioni - L'articolo 163 stabilisce che chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da 20.000 euro a 120.000 euro.

[5] Doc. web n. 993385 del 23 aprile 2004, con il quale l'Ufficio del Garante ha fornito alcuni chiarimenti per il settore privato (imprese, banche, assicurazioni, professionisti, enti *no-profit*) su altri trattamenti che non devono essere notificati in base ad una corretta interpretazione delle disposizioni del Codice sulla privacy.

Nei casi di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi sopra indicati sono applicati in misura pari a due quinti.

L’articolo 168 del Codice, infine, sanziona le dichiarazioni o le attestazioni false inserite all’interno delle notificazioni con la reclusione da sei mesi a tre anni, salvo che il fatto costituisca più grave reato.

il trasferimento di dati personali all’estero

L’articolo 43 del Codice prevede che il trasferimento, anche temporaneo, fuori del territorio nazionale, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, qualora sia diretto verso un Paese extra UE è consentito in alcune ipotesi, tra cui quando:

- l'interessato abbia manifestato il proprio consenso espresso ovvero, in caso di dati sensibili, in forma scritta;
- sia necessario per l'esecuzione di obblighi contrattuali o precontrattuali;
- sia necessario per la salvaguardia di un interesse pubblico.

le garanzie per i dati sensibili

Sono definiti come “dati sensibili” dall’articolo 4 del Codice sulla privacy i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale.

La normativa intende assicurare ai dati personali sensibili maggiore protezione rispetto ai normali dati personali. Infatti, l’articolo 26 del Codice stabilisce che i dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell’osservanza delle prescrizioni del Codice e delle norme vigenti.

L’articolo 26 prevede in alcuni casi la possibilità di trattare i dati sensibili anche senza consenso dell’interessato, ma con l’autorizzazione del Garante, tra i quali:

- quando si tratta di dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria;
- quando si tratta di dati contenuti nei curricula spontaneamente trasmessi dagli interessati al fine dell’eventuale instaurazione di un rapporto di lavoro;
- quando il trattamento è effettuato da associazioni senza scopo di lucro, anche non riconosciute, a carattere politico, filosofico, religioso o sindacale relativamente ai dati personali degli aderenti o dei soggetti che in relazione alle finalità dell’associazione hanno contatti regolari con essa, sempre che i dati non siano comunicati o diffusi fuori del relativo ambito e l’ente, l’associazione o l’organismo determinino idonee garanzie relativamente ai trattamenti effettuati;
- quando il trattamento è necessario per la salvaguardia della vita o dell’incolumità fisica dell’interessato o di un terzo nel caso in cui l’interessato non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità d’intendere o di volere;
- quando il trattamento è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza.

I dati idonei a rivelare lo stato di salute non possono comunque essere diffusi.

L’articolo 26 del Codice richiede inoltre per il trattamento di dati sensibili un vero e proprio atto autorizzatorio da parte dell’Autorità Garante.

La disposizione ha la finalità di assicurare maggiore attenzione verso quei dati suscettibili di creare discriminazioni di vario tipo nei confronti dei soggetti interessati. Ma per evitare il rischio di congestionare l’Ufficio del Garante con milioni di richieste da evadere, pena la completa paralisi dell’attività di ogni impresa, ente o associazione, l’articolo 40 del Codice consente al Garante l’emanazione di provvedimenti autorizzatori cosiddetti “cumulativi”.

Il Garante ha già provveduto ad emanare alcuni provvedimenti con cui sostanzialmente sono stati autorizzati, con l’adozione di opportune cautele, una serie di trattamenti tipici di dati sensibili per alcune categorie di titolari.

Tali provvedimenti hanno generalmente validità limitata, annuale o poco più, e autorizzano implicitamente i trattamenti ivi contemplati che si conformino alle prescrizioni stabilite.

Con l'autorizzazione n. 5 dell'11 dicembre 2014[6] il Garante ha legittimato il trattamento dei dati sensibili, fatta eccezione per quelli idonei a rivelare la vita sessuale, effettuato da parte delle imprese che operano nel settore turistico o alberghiero o del trasporto, agenzie di viaggio e operatori turistici.

L'autorizzazione legittima i trattamenti indispensabili per adempiere agli obblighi, anche precontrattuali, che tali imprese assumono nel proprio settore di attività, al fine di fornire specifici beni, prestazioni, o servizi richiesti dall'interessato. Legittima inoltre i trattamenti effettuati per adempiere, o per esigere l'adempimento, ad obblighi di natura fiscale e contabile, o imposti da norme comunitarie, dalla legge, dai regolamenti, o dai contratti collettivi, o prescritti da autorità o organi di vigilanza o di controllo nei casi indicati dalla legge o dai regolamenti.

Sono infatti autorizzati i trattamenti di dati sensibili relativi ai soggetti ai quali sono forniti i beni, le prestazioni o i servizi, se tali dati sono pertinenti rispetto a quanto specificamente richiesto da tale soggetto, che deve comunque manifestare il suo consenso scritto ed informato. Allo stesso modo è possibile trattare dati sensibili di terzi, quando non sia possibile procedere alla fornitura al beneficiario dei beni, delle prestazioni o dei servizi.

I dati sensibili possono essere comunicati a soggetti pubblici o privati, ivi compresi fondi e casse di previdenza ed assistenza, nonché, ove necessario, ai familiari dell'interessato, nei limiti strettamente pertinenti al perseguimento delle finalità per le quali è consentito il trattamento.

Le imprese titolari di tali trattamenti devono conservare un elenco dei destinatari delle comunicazioni di dati sensibili effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

Non è consentita la diffusione di tali dati sensibili.

Per quanto riguarda le modalità del trattamento, oltre al rispetto delle specifiche disposizioni del Codice e dell'Allegato B, che analizzeremo in seguito, l'autorizzazione richiede che il trattamento dei dati sensibili venga effettuato unicamente con operazioni, con logiche e con forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità sopra indicate. La comunicazione di tali dati all'interessato deve avvenire di regola direttamente a quest'ultimo o ad un suo delegato (tranne i casi previsti dall'articolo 82, comma 2, lettera a) del Codice: e cioè impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, eccetera).

Per quanto riguarda invece la conservazione, l'autorizzazione prescrive che i dati sensibili possano essere conservati per un periodo non superiore a quello necessario per perseguire le finalità, ovvero per adempiere agli obblighi o agli incarichi sopra menzionati.

L'autorizzazione n. 5/2014 ha efficacia a decorrere dal 1° gennaio 2015 fino al 31 dicembre 2016.

Con l'autorizzazione n. 1 dell'11 dicembre 2014[7] il Garante ha invece legittimato il trattamento di dati sensibili finalizzato alla gestione dei rapporti di lavoro.

---

[6] Pubblicata sulla Gazzetta Ufficiale n. 301 del 30 dicembre 2014 - doc. web n. 3620455.

[7] Pubblicata sulla Gazzetta Ufficiale n. 301 del 30 dicembre 2014 - doc. web n. 3619884

Tale autorizzazione è rilasciata ai datori di lavoro persone fisiche e giuridiche, imprese, enti, associazioni, eccetera, che sono parte di un rapporto di lavoro o che utilizzano prestazioni lavorative anche atipiche, parziali o temporanee, o che comunque conferiscano un incarico professionale.

Il trattamento può riguardare i dati sensibili attinenti:

- a lavoratori dipendenti, anche se prestatori di lavoro temporaneo o in rapporto di tirocinio, apprendistato e formazione e lavoro, ovvero ad associati anche in compartecipazione e, se necessario, ai dati attinenti ai relativi familiari e conviventi;
- a consulenti e a liberi professionisti, ad agenti, rappresentanti e mandatari;
- a soggetti che effettuano prestazioni coordinate e continuative o ad altri lavoratori autonomi in rapporto di collaborazione;
- a candidati all'instaurazione dei rapporti di lavoro di cui sopra;
- a persone fisiche che ricoprono cariche sociali o altri incarichi nelle persone giuridiche, negli enti, nelle associazioni e negli organismi in cui in cui è organizzato il datore di lavoro;
- a terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui sopra.

Il trattamento dei dati sensibili deve essere indispensabile:

- per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa comunitaria, da leggi, da regolamenti o da contratti collettivi anche aziendali, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia di igiene e sicurezza del lavoro o della popolazione, nonché in materia fiscale, sindacale, di tutela della salute, dell'ordine e della sicurezza pubblica;
- anche fuori dei casi di cui sopra, è consentito il trattamento di dati sensibili in conformità alla legge e per scopi determinati e legittimi, ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti, liberalità o benefici accessori;
- per perseguire finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo;
- per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalle leggi, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
- per esercitare il diritto di accesso ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia;
- per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di igiene e di sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;

- per garantire le pari opportunità;
- per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.

I dati sensibili devono essere strettamente pertinenti ai suddetti obblighi, compiti o finalità, sempreché non sia possibile l'utilizzo di dati anonimi o di dati personali di natura diversa. Nel rispetto di questa limitazione, il Garante consente il trattamento:

- dei dati sensibili concernenti la fruizione di permessi e festività religiose o di servizi particolari di mensa, nonché la manifestazione, nei casi previsti dalla legge, dell'obiezione di coscienza;
- dei dati sensibili concernenti l'esercizio di funzioni pubbliche e di incarichi politici, di attività o di incarichi sindacali (sempre che il trattamento sia effettuato ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali), ovvero l'organizzazione di pubbliche iniziative, nonché dei dati inerenti alle trattenute per il versamento delle quote di servizio sindacale o delle quote di iscrizione ad associazioni od organizzazioni politiche o sindacali;
- dei dati sensibili raccolti e ulteriormente trattati in riferimento a invalidità, infermità, gravidanza, puerperio o allattamento, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psico-fisica a svolgere determinate mansioni, all'appartenenza a determinate categorie protette, nonché dei dati contenuti nella certificazione sanitaria attestante lo stato di malattia, anche professionale dell'interessato, o comunque relativi anche all'indicazione della malattia come specifica causa di assenza del lavoratore.

Restano fermi gli obblighi di informare l'interessato e, ove necessario, di acquisirne il consenso scritto, in conformità a quanto previsto dagli articoli 13, 23 e 26 del Codice. Restano anche ferme le prescrizioni relative alle modalità di trattamento e alla conservazione dei dati previste dal Codice, dall'Allegato B, nonché dall'autorizzazione n. 5/2014.

L'autorizzazione n. 1/2014 ha efficacia a decorrere dal 1° gennaio 2015 fino al 31 dicembre 2016.

le sanzioni – L'articolo 167 prevede che, salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, proceda al trattamento di dati personali sensibili in violazioni alle prescrizioni relative al consenso, sempreché dal fatto derivi nocumento, sia punito con la reclusione da uno a tre anni.

L'articolo 170, infine, sanziona colui che non osserva le misure e gli accorgimenti stabiliti dal Garante all'interno dei provvedimenti autorizzatori con la reclusione da tre mesi a due anni.

le deleghe di responsabilità ed il conferimento di incarichi

L'articolo 29 del Codice stabilisce che il responsabile del trattamento, qualora designato, deve essere un soggetto, persona fisica o persona giuridica, che "per esperienza, capacità ed affidabilità" fornisca idonea garanzia del rispetto delle vigenti disposizioni in materia di privacy, ivi compreso il profilo della sicurezza.

La nomina di un responsabile non è pertanto obbligatoria, ma qualora il titolare intenda avvalersi della collaborazione di un soggetto, dovrà effettuare una scelta oculata. Né potrebbe essere altrimenti, vista l'entità delle sanzioni, anche penali, che comunque la legge pone a carico del titolare, salvo ovviamente dimostrare la completa assenza di responsabilità.

La normativa richiede inoltre che il conferimento dell'incarico al responsabile avvenga per iscritto, specificando analiticamente i compiti a lui affidati. Il responsabile deve quindi attenersi alle istruzioni impartite dal titolare, il quale, anche con verifiche periodiche, è tenuto a vigilare sulla puntuale osservanza delle disposizioni di legge e delle proprie istruzioni. Pertanto, la delega di funzioni da parte del titolare non esonera il titolare stesso dall'onere di sorvegliare l'andamento delle operazioni di trattamento svolte dal responsabile.

Per le realtà organizzative complesse, il Codice prevede la possibilità di nominare responsabili più soggetti, anche mediante suddivisione di compiti.

Il titolare ed il responsabile sono quindi le figure apicali, mentre tutti gli altri soggetti da loro preposti nel trattamento di dati personali assumono il ruolo di incaricati. L'articolo 30 del Codice prevede infatti che gli incaricati al trattamento, designati per iscritto, debbano procedere alle elaborazioni di dati personali ai quali hanno accesso attendendosi alle istruzioni del titolare o del responsabile.

Possono essere designati quali incaricati del trattamento solo ed esclusivamente persone fisiche, e non anche le entità personificate che possono invece rivestire la qualità di responsabile del trattamento.

In proposito, occorre sottolineare che, interpretando la definizione data dall'articolo 4, primo comma, lettera l) del Codice, non può essere considerata "comunicazione" la conoscenza dei dati personali da parte delle persone incaricate per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta autorità.

Nel prevedere la figura dell'incaricato del trattamento la normativa ha inteso evitare che i collaboratori del titolare siano considerati quali "terzi" ai fini dell'applicazione delle disposizioni sulla protezione dei dati personali.

Infatti, non sono considerati terzi gli incaricati del trattamento previamente individuati per iscritto e che operano sotto la diretta autorità del titolare o del responsabile, attuandone le istruzioni.

Gli incaricati possono coadiuvare il titolare sia operando all'interno dell'ordinaria struttura del titolare, sia operando presso un centro esterno.

Ricordiamo che la designazione deve essere effettuata per iscritto e deve individuare puntualmente l'ambito del trattamento consentito all'incaricato. Si considera comunque tale anche la documentata preposizione della persona fisica ad una unità, per

la quale è individuato, per iscritto, l’ambito del trattamento consentito agli addetti all’unità medesima.

le modalità di raccolta e requisiti dei dati

Secondo l’articolo 11 della Codice sulla privacy, i dati personali oggetto di trattamento devono essere:

a) trattati in modo lecito e corretto;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Tra i criteri elencati, è evidente la rilevanza che il Legislatore ha voluto riservare al principio di finalità, che trova compiuta espressione nella lettera b). Come in più occasioni anche il Garante ha avuto modo di sottolineare, riveste considerevole importanza la modalità di raccolta e registrazione dei dati, che deve essere effettuata per scopi determinati, espliciti e legittimi. I dati, inoltre, non possono essere utilizzati in altre operazioni del trattamento incompatibili con tali scopi.

Occorre infatti tenere a mente che una delle più gravi lesioni del diritto alla riservatezza delle persone nel trattamento dei dati risiede proprio nel potenziale loro uso distorto rispetto a ciò che viene dichiarato.

Il rispetto delle finalità dichiarate nel momento nel quale il dato viene raccolto rappresenta quindi la base fondamentale sulla quale il diritto alla riservatezza può concretamente essere costruito.

le misure di sicurezza

L'articolo 31 del Codice stabilisce che i dati personali oggetto di trattamento debbano essere custoditi e controllati mediante l'adozione di idonee e preventive 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.

Il Codice definisce come "misure minime" quel complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione normativamente richiesto rispetto ai rischi sopraelencati.

Le misure di sicurezza variano in relazione alla natura dei dati ed alle specifiche caratteristiche del trattamento, e potranno essere modificate dal Garante in relazione alle conoscenze acquisite con il progresso tecnico.

A livello internazionale[8] si è concordi nel ritenere che le misure di sicurezza, per essere efficaci, devono garantire il raggiungimento dei seguenti obiettivi:

- salvaguardare la riservatezza, ossia prevenire l'utilizzo indebito di informazioni riservate. In pratica eliminare, o quanto meno ridurre a livelli accettabili, il rischio che un soggetto non autorizzato possa utilizzare un'informazione altrui, e quindi controllare l'accesso alle informazioni attraverso adeguate misure di protezione;
- garantire l'integrità, ovvero prevenire l'alterazione o manipolazione indebita delle informazioni. Eliminare quindi o ridurre a livelli accettabili il rischio di cancellazioni o modifiche dei dati, a seguito di guasti, interruzione nella somministrazione di energia elettrica, incendi, allagamenti, etc. o di interventi da parte di soggetti non autorizzati;
- garantire la disponibilità, e cioè la possibilità di accesso, controllato, alle informazioni. Occorre infatti prevenire i pericoli di occultamento o di impossibilità di accesso a dati o risorse necessarie alla conduzione di un'attività lecita.

La concrete misure di sicurezza che i titolari di trattamenti di dati personali, sensibili o non sensibili, automatizzati o manuali, sono tenuti ad adottare sono individuate negli articoli da 33 a 36 del Codice sulla privacy e nel disciplinare tecnico contenuto nell'Allegato B.

Per quanto riguarda le aziende ricettive, nei prossimi capitoli abbiamo sintetizzato e classificato gli adempimenti in materia di sicurezza sulla base delle modalità con cui viene effettuato il trattamento e del tipo di dati.

Dalla lettura dell'articolo 31 del Codice risulta comunque evidente la volontà del legislatore di garantire che il trattamento di dati personali non costituisca oggetto di abusi.

Il Legislatore si preoccupa costantemente di garantire che l'intromissione nella sfera privata di un soggetto, necessaria per la formazione di una banca dati, venga equamente bilanciata dal rispetto di principi di garanzia e da uno specifico iter procedimentale, la cui osservanza viene rafforzata mediante appunto la previsione di idonee misure di sicurezza, elencate nel disciplinare tecnico contenuto nell'Allegato B del Codice, di seguito riassunte.

[8] Decisione del Consiglio d'Europa del 31 marzo 1992; Raccomandazione OCSE sulle "linee direttrici relative alla sicurezza dei sistemi d'informazione" del 26 novembre 1992; Libro verde sulla sicurezza dei sistemi informativi elaborato dalla Commissione Europea il 14 luglio 1994.

il trattamento senza l'ausilio di strumenti elettronici di dati personali non sensibili - Ad esempio: dati dei clienti trattati ai fini della notifica alla polizia o ad altri fini connessi con il servizio di alloggio, ricevute fiscali, fatture, mailing list utilizzate per fini promozionali, altri documenti relativi ai fornitori o ai lavoratori, purché non contenenti dati sensibili (sono considerati dati sensibili ad esempio l'adesione a sindacati o i certificati di malattia), eccetera:

- il titolare o, se designato, il responsabile, devono designare per iscritto gli incaricati del trattamento;
- gli incaricati procedono al trattamento attenendosi alle istruzioni scritte impartite dal titolare o dal responsabile, finalizzate al controllo e alla custodia degli atti e dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento del trattamento dei dati.

il trattamento senza l'ausilio di strumenti elettronici di dati personali sensibili - Ad esempio: dati sull'adesione dei lavoratori a sindacati o su loro malattie o invalidità, eccetera:

- il titolare o, se designato, il responsabile, devono designare per iscritto gli incaricati del trattamento;
- gli incaricati procedono al trattamento attenendosi alle istruzioni scritte impartite dal titolare o dal responsabile, finalizzate al controllo e alla custodia degli atti e dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento del trattamento dei dati;
- l'accesso agli archivi contenenti dati sensibili dovrà essere controllato e le persone ammesse dopo l'orario di chiusura identificate e registrate.

il trattamento con strumenti elettronici di dati personali non sensibili - Ad esempio: dati dei clienti trattati ai fini della notifica alla polizia e ad altri fini connessi con il servizio di alloggio, ricevute fiscali, fatture, mailing list utilizzate per fini promozionali, altri documenti relativi ai fornitori o ai lavoratori, purché non contenenti dati sensibili (sono considerati dati sensibili ad esempio l'adesione a sindacati o i certificati di malattia) eccetera:

- il titolare o, se designato, il responsabile, devono designare per iscritto gli incaricati del trattamento;
- l'incaricato procede al trattamento attenendosi alle istruzioni scritte impartite dal titolare o dal responsabile; l'accesso al trattamento di determinate informazioni avviene solo in caso di assoluta necessità in ragione della sua attività e dopo aver superato un duplice controllo, che consiste in una verifica di autenticazione (codice identificativo e parola chiave, quest'ultima da modificare ogni 6 mesi), al fine di poter utilizzare l'apparecchiatura elettronica, ed in una verifica di autorizzazione, al fine di poter utilizzare attraverso l'apparecchiatura una determinata applicazione informatica destinata al trattamento delle informazioni;
- il titolare del trattamento è tenuto a proteggere i dati attivando idonei strumenti elettronici da aggiornare almeno semestralmente. E' inoltre tenuto ad aggiornare annualmente i programmi volti a prevenire la vulnerabilità degli strumenti elettrici ed a correggerne i difetti. Vanno infine impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;
- nel caso in cui il titolare adotti le misure di sicurezza avvalendosi di soggetti esterni

alla propria struttura, dovrà ricevere dall'installatore una descrizione scritta degli interventi che ne attesti al conformità al disciplinare tecnico del Codice.

il trattamento con strumenti elettronici di dati personali sensibili - Ad esempio: dati sull'adesione a sindacati da parte dei lavoratori o su loro malattie o invalidità, eccetera, vanno applicate le stesse misure di sicurezza previste per i trattamenti di dati personali non sensibili, con alcune peculiarità sotto riportate:

- la parola chiave deve essere modificata dall'incaricato al primo utilizzo e successivamente almeno ogni 3 mesi (anziché ogni 6 mesi come nel caso di trattamento di dati non sensibili);
- anche i dati sensibili vanno protetti attivando idonei strumenti elettronici da aggiornare almeno semestralmente, ma i programmi volti a prevenire la vulnerabilità degli strumenti elettrici ed a correggerne i difetti vanno aggiornati semestralmente, anziché annualmente come per i dati personali non sensibili;
- vanno impartite apposite istruzioni per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e tali supporti, se non utilizzati, dovranno essere distrutti;
- occorre prevedere degli interventi formativi per gli incaricati del trattamento, sia per renderli edotti sui rischi che incombono sui dati, sia sulle misure disponibili per prevenire eventi dannosi.

le sanzioni – L'articolo 169 sanziona la mancata adozione delle misure minime di sicurezza come illecito penale punibile con l'arresto sino a due anni. L'autore del reato potrà avvalersi del cosiddetto ravvedimento operoso che dovrà essere adottato seguendo correttamente le prescrizioni impartite dal Garante. L'adempimento e il pagamento di un'ammenda ridotta estinguono il reato.

la semplificazione di adempimenti relativi alle misure di sicurezza

Il Garante, con proprio provvedimento[9], ha provveduto a semplificare le disposizioni relative alle misure minime di sicurezza per i soggetti che:

- utilizzano dati personali non sensibili (ad esempio nome, cognome, indirizzo, codice fiscale, numero di telefono) o che trattano come unici dati sensibili riferiti ai propri dipendenti e collaboratori, anche a progetto, quelli costituiti dallo stato di salute o malattia senza indicazione della relativa diagnosi, ovvero dall'adesione a organizzazioni sindacali o a carattere sindacale;
- trattano dati personali unicamente per correnti finalità amministrative e contabili, in particolare presso liberi professionisti, artigiani e piccole e medie imprese.

Tra le categorie di cui sopra rientrano sicuramente le aziende ricettive, tranne quelle che trattano dati sensibili (attinenti alla salute, alle idee politiche o religiose, alla razza, eccetera) diversi da quelli relativi allo stato di salute dei dipendenti o collaboratori o attinenti alla loro adesione ad organizzazioni sindacali.

il trattamento senza l'ausilio di strumenti elettronici - Le misure minime di sicurezza semplificate sono di seguito individuate:

- impartire agli incaricati, anche oralmente, istruzioni finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
- quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dai medesimi incaricati fino alla restituzione in modo che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

il trattamento con strumenti elettronici – Sono previste le seguenti misure semplificate:

- le istruzioni in materia di misure minime di sicurezza previste dall'Allegato B del Codice possono essere impartite agli incaricati del trattamento anche oralmente, con indicazioni di semplice e chiara formulazione;
- per l'accesso ai sistemi informatici si può utilizzare un qualsiasi sistema di autenticazione basato su un codice per identificare chi accede ai dati (di seguito, "username"), associato a una parola chiave (di seguito: "password"), in modo che:
  - ⇒ l'username individui in modo univoco una sola persona, evitando che soggetti diversi utilizzino codici identici;
  - ⇒ la password sia conosciuta solo dalla persona che accede ai dati.

[9] Provvedimento del 27 novembre 2008, G.U. n. 287 del 9.12.2008 – doc web n. 1571218

L'username deve essere disattivato quando l'incaricato non ha più la qualità che rende legittimo l'utilizzo dei dati (ad esempio, in quanto non opera più all'interno dell'organizzazione).

Può essere adottata, quale procedura di autenticazione anche la procedura di login disponibile sul sistema operativo delle postazioni di lavoro connesse a una rete.

Il titolare deve definire le procedure e le modalità con cui, in caso di necessità, potrà accedere ai dati o agli strumenti elettronici in caso di prolungata assenza dell'incaricato (ad esempio, prescrivendo ai lavoratori che si assentino dall'ufficio per ferie l'attivazione di modalità che consentano di inviare automaticamente messaggi di posta elettronica ad un altro recapito accessibile[10]. L'incaricato deve essere informato degli interventi effettuati;

- qualora sia necessario diversificare l'ambito del trattamento consentito, possono essere assegnati agli incaricati, singolarmente o per categorie omogenee, corrispondenti profili di autorizzazione, tramite un sistema di autorizzazione o funzioni di autorizzazione incorporate nelle applicazioni software o nei sistemi operativi, così da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento;
- i soggetti di cui alla premessa devono assicurare che l'ambito di trattamento assegnato ai singoli incaricati, nonché agli addetti alla gestione o alla manutenzione degli strumenti elettronici, sia coerente con i principi di adeguatezza, proporzionalità e necessità, anche attraverso verifiche periodiche, provvedendo, quando è necessario, ad aggiornare i profili di autorizzazione eventualmente accordati.

  I programmi di sicurezza (antivirus) devono essere aggiornati almeno una volta l'anno (biennalmente se il computer non è connesso alla rete Internet), ed il backup dei dati deve essere effettuato almeno una volta al mese.

.

[10] Vedi le "Linee guida in materia di lavoro per posta elettronica e Internet" approvate dal Garante, doc. web n. 1387522.

l'amministratore di sistema

Con un provvedimento del 2008[11], modificato nel 2009[12], il Garante della Privacy ha voluto segnalare a tutti i titolari di trattamenti di dati personali, effettuati con strumenti elettronici, la particolare criticità del ruolo degli amministratori di sistema.

Il provvedimento richiama l'attenzione dei titolari di trattamenti di dati personali sulla necessità di:

- adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di amministratore di sistema;
- valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali.

Il Garante ha successivamente provveduto ad emanare alcuni chiarimenti[13] in ordine alle prescrizioni impartite in materia di amministratori di sistema, anche allo scopo di evitare ingiustificati oneri per le aziende:

- le prescrizioni riguardano solo quei soggetti che, nel trattare i dati personali con strumenti informatici, devono ricorrere o abbiano fatto ricorso alla figura professionale dell'amministratore di sistema o a una figura equivalente;
- le prescrizioni non si applicano, invece, a quei soggetti anche di natura associativa che, generalmente dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi, possano fare a meno di una figura professionale specificamente dedicata alla amministrazione dei sistemi o comunque abbiano ritenuto di non farvi ricorso;
- per quanto concerne, infine, gli aspetti tecnici del provvedimento (in particolare, la conservazione dei log degli accessi effettuati dagli amministratori di sistema), il Garante ha ricordato che l'adeguamento può avvenire anche con soluzioni a basso costo, validamente proposte e disponibili in rete (per esempio basate su software gratuito, anche con licenze di tipo open source), che possono costituire valide alternative all'impiego di prodotti commerciali o di apparati più sofisticati.

Pertanto, i titolari di trattamenti di dati personali diversi da quelli effettuati a fini amministrativo-contabili che ricorrono alla figura professionale dell'amministratore di sistema, o a figure analoghe, devono ottemperare alle prescrizioni che seguono.

valutazione delle caratteristiche soggettive - L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. E' comunque possibile nominare un amministratore di

[11] Provvedimento del 27 novembre 2008, G.U. n. 300 del 24 dicembre 2008 - doc. web n. 1577499

[12] Provvedimento del 25 giugno 2009, G.U. n. 149 del 30 giugno 2009 - doc. web n. 1626595.

[13] Comunicato stampa del 10.12.2009, doc web n.1676654

sistema semplicemente come incaricato del trattamento ma, in questo caso, va comunque seguita la stessa procedura e valutazione dei requisiti che si fa in caso di nomina di un responsabile.

designazioni individuali - La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

elenco degli amministratori di sistema - Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante. Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i lavoratori hanno diritto di essere informati, con modalità diverse a scelta del datore di lavoro, sull'identità degli amministratori di sistema.

servizi in outsourcing - Nel caso di servizi di amministrazione di sistema affidati in outsourcing, il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

verifica delle attività - L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

registrazione degli accessi - Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

la comunicazione elettronica

Il titolo X del Codice, articoli da 121 a 134, regolamenta la complessa questione della tutela dei dati personali nell'ambito della comunicazione elettronica.

Gli strumenti automatizzati e telematici hanno ormai una diffusione enorme. Senza pensare alle forme più evolute di comunicazione elettronica, anche lo stesso uso del telefono o del fax può potenzialmente mettere a rischio la riservatezza delle informazioni, e necessita quindi di cautele.

Garantire la sicurezza delle informazioni diventa però sempre più difficile dal momento che la tecnologia evolve continuamente consentendo sempre più sofisticate metodologie di raccolta e trattamento di dati personali.

Il Codice si preoccupa di fissare regole ben precise a carico dei fornitori di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione. Le prescrizioni sono quindi rivolte a chi fornisce il servizio, e non quindi all'impresa ricettiva che in tale fattispecie è considerata come destinataria delle garanzie previste dal Codice.

Poiché però l'impresa ricettiva a sua volta spesso consente l'utilizzo dei propri sistemi di comunicazione elettronica ai clienti, potrebbe in alcune ipotesi essere considerata essa stessa come fornitrice del servizio, e quindi tenuta al rispetto di alcune regole basilari in tema di riservatezza delle informazioni.

Il Codice tende comunque a garantire comunicazioni riservate e sicure, impedendo inoltre le chiamate telefoniche, fax pubblicitari o messaggi indesiderati ed i trasferimenti di chiamata inopportuni, e riconosce anche il diritto degli utenti a non essere inseriti negli elenchi o a far omettere l'indirizzo negli elenchi stessi.

Il Codice prevede inoltre che il fornitore del servizio di telecomunicazioni tratti i dati relativi alla fatturazione entro stretti limiti oggettivi e cronologici, ed attenendosi a particolari cautele.

Sintetizziamo di seguito alcune delle più rilevanti disposizioni:

dati sul traffico e fatturazione - I dati sul traffico relativo ai contraenti ed utenti, trattati dal fornitore del servizio di comunicazione elettronica, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione elettronica.

I dati possono però essere sottoposti a trattamento ai fini della fatturazione all'utente solo per un periodo di tempo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per far fronte ad eventuali contestazioni anche in sede giudiziale (non oltre il termine di prescrizione del credito).

I dati relativi al traffico telefonico sono conservati dal fornitore per 24 mesi, per finalità di accertamento e repressione di reati, mentre per le stesse finalità i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per 12 mesi dalla data della comunicazione.

I dati possono invece essere soggetti a trattamento ai fini di commercializzazione e promozione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto solo se l'utente ha dato il consenso.

In ogni caso il trattamento dei dati relativi al traffico ed alla fatturazione è consentito unicamente agli incaricati che agiscono sotto la diretta autorità del fornitore del servizio.

Gli utenti hanno diritto di ricevere una fatturazione dettagliata, ma in ogni caso le ultime tre cifre dei numeri chiamati devono essere omesse.

Il fornitore del servizio è tenuto comunque ad abilitare l'utente ad effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente ed in modo agevole, avvalendosi per il pagamento di modalità alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate.

identificazione della linea - Se è disponibile l'identificazione della linea chiamante, l'utente chiamante deve avere la possibilità, gratuitamente e mediante una funzione semplice, di impedire tale identificazione.

L'utente chiamato deve avere invece la possibilità, gratuitamente e mediante una funzione semplice, di respingere le chiamate anonime.

chiamate di disturbo – L'utente che riceve chiamate di disturbo potrà richiedere l'identificazione delle chiamate per un periodo non superiore a quindici giorni, a proprie spese e previa domanda scritta al fornitore del servizio, eventualmente preceduta in caso di urgenza da una richiesta telefonica.

trasferimento automatico della chiamata - Il fornitore del servizio deve adottare le misure necessarie per consentire a ciascun utente, gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico verso il proprio terminale delle chiamate da parte dei terzi.

comunicazioni indesiderate - L'uso di sistemi automatizzati di chiamata senza intervento di un operatore per scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale è consentito solo con il consenso dell'interessato.

Tale disposizione si applica anche alle comunicazioni effettuate per gli stessi scopi mediante posta elettronica, telefax, messaggi mms o sms o di altro tipo. L'uso di altri mezzi per tali scopi è invece consentito ai sensi degli articoli 23 e 24 del Codice.

Se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita o del servizio, e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni.

riservatezza - Il fornitore di un servizio di telecomunicazione deve informare gli utenti, qualora ci sia la possibilità che soggetti ad esso estranei ascoltino non intenzionalmente il contenuto di comunicazioni o conversazioni.

L'utente deve informare gli altri utenti quando nel corso della conversazione vengano utilizzati dispositivi che consentano l'ascolto della conversazione ad altri soggetti (viva voce, comunicazione a tre).

LE LINEE GUIDA DEL GARANTE

la gestione del rapporto di lavoro

Allo scopo di fornire indicazioni e raccomandazioni ai datori di lavoro del settore privato sulle operazioni di trattamento di dati personali, anche sensibili, dei lavoratori, il Garante ha emanato alcune specifiche linee guida[14].

Di seguito, una sintesi del provvedimento.

tipologie di trattamenti - Nell'ambito dei rapporti di lavoro, i trattamenti effettuati dal datore di lavoro riguardano normalmente i dati anagrafici dei lavoratori, nonché altre informazioni connesse allo svolgimento dell'attività lavorativa (la tipologia del contratto, la qualifica, la retribuzione, il tempo di lavoro anche straordinario, ferie e permessi, assenza dal servizio, procedimenti disciplinari, eccetera). E' possibile che vengano trattatati dati biometrici e dati sensibili, riferiti anche a terzi (credo religioso, adesione a sindacati, dati che rivelano lo stato di salute contenuti in certificati medici o in altra documentazione).

rispetto dei principi di protezione dei dati personali - I dati personali del lavoratore possono essere trattati dal datore di lavoro nella misura in cui ciò sia necessario per dare corretta esecuzione al rapporto di lavoro. Le informazioni trattate devono essere pertinenti e non eccedenti le finalità perseguite, e devono essere osservate tutte le disposizioni del Codice della privacy:

- rispetto dei principi di necessità e liceità (artt. 3 e 11);
- obbligo di fornire ai dipendenti un'adeguata informativa (art. 13);
- richiesta preventiva del consenso nei casi in cui il trattamento non sia conseguenza necessaria del contratto di lavoro, o non sia imposto da leggi, regolamenti, contratti e accordi collettivi (artt. 23, 24, 26 e 43 del Codice); ricordiamo che l'articolo 26 consente, con alcuni limiti, di trattare senza consenso anche i dati sensibili del lavoratore, quando ciò sia necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza;
- rispetto delle prescrizioni impartite dal Garante, anche nelle autorizzazioni di carattere generale (artt. 26 e 27 del Codice; autorizzazione generale n. 1/2014[15]) per il trattamento di dati sensibili o giudiziari;
- adozione delle misure di sicurezza idonee a preservare i dati da alcuni eventi, tra i quali accessi ed utilizzazioni indebite, rispetto ai quali il datore di lavoro può essere chiamato a rispondere civilmente e penalmente (artt. 15, 31 e ss., 167 e 169 del Codice).

titolare e responsabile - Le linee guida richiamano l'attenzione sulla necessità di identificare le figure soggettive che, a diverso titolo, possono trattare i dati, definendo chiaramente le rispettive attribuzioni, in particolare quelle del titolare e del responsabile.

[14] Provvedimento n. 53 del 23 novembre 2006, GU n. 285 del 7.12.2006 - doc. web n. 1364939.

[15] Pubblicata sulla Gazzetta Ufficiale n. 301 del 30 dicembre 2014 - doc. web n. 3619884

Nelle realtà imprenditoriali più articolate l'identificazione spesso non risulta agevole, ostacolando l'esercizio dei diritti dei lavoratori.

Nell'ambito dei gruppi di imprese, le società controllate e collegate possono delegare la società capogruppo a svolgere adempimenti in materia di lavoro, previdenza ed assistenza sociale per i lavoratori: tale attività implica la designazione della società capogruppo quale responsabile del trattamento ai sensi dell'art. 29 del Codice. Analoga soluzione deve essere adottata per i consorzi di società cooperative, nei quali a tal fine può essere designata una delle società consorziate.

medico competente – Il medico competente effettua accertamenti preventivi e periodici sui lavoratori e istituisce, curandone l'aggiornamento, una cartella sanitaria e di rischio. Detta cartella è custodita presso l'azienda, con salvaguardia del segreto professionale, e consegnata in copia al lavoratore al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne faccia richiesta. Il medico competente è quindi deputato a trattare i dati sanitari dei lavoratori, procedendo alle dovute annotazioni nelle cartelle sanitarie e di rischio, e curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate. Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali aziendali (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti) con salvaguardia del segreto professionale. Il datore di lavoro è tenuto ad adottare le misure preventive e protettive per i lavoratori, su parere del medico competente o qualora il medico lo informi di anomalie imputabili all'esposizione a rischio, ma non può conoscere le eventuali patologie accertate, ma solo la valutazione finale circa l'idoneità del dipendente, dal punto di vista sanitario, allo svolgimento di date mansioni.

dati biometrici e accesso ad "aree riservate" - L'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito. Tali dati, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta, partendo dal modello di riferimento, e la sua ulteriore "utilizzazione" a loro insaputa. L'utilizzo di dati biometrici può essere giustificato solo in casi particolari, per presidiare accessi ad "aree sensibili" (processi produttivi pericolosi o sottoposti a segreti di varia natura, o per locali destinati alla custodia di beni o documenti segreti o riservati o di valore). Inoltre, nei casi in cui l'uso dei dati biometrici è consentito, i sistemi informativi devono essere configurati in modo da ridurre al minimo l'utilizzazione di dati personali, e da escluderne il trattamento quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità. Resta salva, per fattispecie particolari o in ragione di situazioni eccezionali, la presentazione di apposito interpello al Garante (art. 17 del Codice) da parte di titolari del trattamento che intendano discostarsi da queste prescrizioni.

comunicazione di dati personali - Il datore di lavoro, qualora non ricorrano le condizioni di cui all'art. 24 del Codice (ad esempio comunicazione di dati a terzi prevista dal contratto di lavoro o da leggi, regolamenti, contratti e accordi collettivi) deve chiedere il consenso al lavoratore per comunicare i suoi dati a terzi (associazioni di datori di lavoro o di ex dipendenti; conoscenti, familiari e parenti).

Non costituisce comunicazione a terzi la conoscenza dei dati da parte dei soggetti, interni o esterni, incaricati del trattamento da parte del datore di lavoro. Infatti, il datore di

lavoro ha piena facoltà di disciplinare le modalità del trattamento, designando i soggetti, interni o esterni, incaricati o responsabili del trattamento, che possono acquisire conoscenza dei dati inerenti alla gestione del rapporto di lavoro, in relazione alle funzioni svolte e a idonee istruzioni scritte alle quali attenersi.

Il datore di lavoro può comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o gruppi di lavoratori.

intranet aziendale - Il consenso del lavoratore è necessario per pubblicare sue informazioni personali (fotografia, informazioni anagrafiche o curriculum) nella intranet aziendale (e a maggior ragione in Internet), non risultando tale ampia circolazione di dati personali di regola necessaria per eseguire obblighi derivanti dal contratto di lavoro (art. 24, comma 1, lett. b, del Codice).

diffusione - In assenza di consenso, o di specifiche disposizioni normative che la impongano o autorizzino, la diffusione di dati personali riferiti ai lavoratori può avvenire solo se necessaria per dare esecuzione a obblighi derivanti dal contratto di lavoro (affissione nella bacheca aziendale di ordini di servizio, di turni lavorativi o feriali, di disposizioni riguardanti l'organizzazione del lavoro e l'individuazione delle mansioni cui sono deputati i singoli dipendenti). Non è invece di regola lecito dare diffusione a informazioni personali di singoli lavoratori, specie se non correlate all'esecuzione di obblighi lavorativi, come ad esempio:

- affissione relativa ad emolumenti percepiti o che fanno riferimento a particolari condizioni personali;
- sanzioni disciplinari irrogate o informazioni relative a controversie giudiziarie;
- assenze dal lavoro per malattia;
- iscrizione e/o adesione dei singoli lavoratori ad associazioni.

cartellini identificativi – Costituisce diffusione di dati personali riportare ed esibire informazioni personali su cartellini identificativi appuntati ad esempio sull'abito o sulla divisa del lavoratore (di solito, con lo scopo di migliorare il rapporto fra operatori ed utenti o clienti). Al riguardo, il Garante ha già rilevato che l'obbligo di portare in modo visibile un cartellino identificativo può trovare fondamento in alcune prescrizioni contenute in accordi sindacali aziendali, il cui rispetto può essere ricondotto alle prescrizioni del contratto di lavoro. Tuttavia, in relazione al rapporto con il pubblico, si è ravvisata la sproporzione dell'indicazione sul cartellino di dati personali identificativi (generalità o dati anagrafici), ben potendo spesso risultare sufficienti altre informazioni (quali codici identificativi, il solo nome o il ruolo professionale svolto), per sé sole in grado di essere d'ausilio all'utenza.

modalità di comunicazione - Il datore di lavoro deve adottare cautele nelle forme di comunicazione con il lavoratore, adottando le misure più opportune per prevenire un'indebita conoscenza di dati personali del lavoratore da parte di terzi (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali).

dati sanitari – Il datore di lavoro deve osservare cautele particolari nel trattamento dei dati sensibili dei lavoratori, e particolarmente di quelli idonei a rivelarne lo stato di salute. Costituisce dato sensibile idoneo a rivelare lo stato di salute del lavoratore l'informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla contestuale enunciazione della diagnosi. Per tali informazioni, oltre alla normativa sulla privacy, anche lo Statuto dei lavoratori richiede particolari accorgimenti per contenere, nei limiti dell'indispensabile, i dati dei quali il datore di lavoro può venire a conoscenza per dare esecuzione al contratto.

assenze per ragioni di salute – La normativa sul lavoro ed i contratti collettivi giustificano il trattamento dei dati relativi ai casi di infermità che determinano un'incapacità lavorativa, temporanea o definitiva, con la conseguente sospensione o risoluzione del contratto. Il datore di lavoro può inoltre trattare dati relativi a invalidità o all'appartenenza a categorie protette, nei modi e per le finalità prescritte dalla vigente normativa in materia. A tale riguardo, infatti, sussiste un quadro normativo articolato che prevede anche l'obbligo del lavoratore di comunicare, e successivamente certificare, al datore di lavoro e all'ente previdenziale lo stato di malattia: obblighi funzionali non solo a giustificare i trattamenti normativi ed economici spettanti al lavoratore, ma anche a consentire al datore di lavoro, nelle forme di legge, di verificare le reali condizioni di salute del lavoratore.

Per attuare tali obblighi viene utilizzata un'apposita modulistica, consistente in un attestato di malattia da consegnare al datore di lavoro (con la sola indicazione dell'inizio e della durata presunta dell'infermità: c.d. "prognosi") e in un certificato di diagnosi da consegnare, a cura del lavoratore stesso, all'INPS o alla struttura pubblica indicata dallo stesso Istituto d'intesa con la regione, se il lavoratore ha diritto a ricevere l'indennità di malattia a carico dell'ente previdenziale.

Tuttavia, qualora dovessero essere presentati dai lavoratori certificati medici con i dati di prognosi e di diagnosi, i datori di lavoro restano obbligati, ove possibile, ad adottare idonee misure e accorgimenti volti a prevenirne la ricezione o, in ogni caso, ad oscurare i dati di diagnosi.

In alcuni casi il datore di lavoro può venire a conoscenza delle condizioni di salute del lavoratore. Nel caso di infortuni o malattie professionali dei lavoratori, ad esempio, la normativa prevede che la denuncia debba essere corredata da specifica certificazione medica. In tal caso, pur essendo legittima la conoscenza della diagnosi, il datore di lavoro deve limitarsi a comunicare all'ente assistenziale esclusivamente le informazioni sanitarie relative o collegate alla patologia denunciata, e non anche dati sulla salute relativi ad altre assenze che si siano verificate nel corso del rapporto di lavoro.

Il datore di lavoro può trattare i dati relativi allo stato di salute del lavoratore, o di suoi congiunti (ad esempio informazioni relative a condizioni di handicap) anche quando ciò è necessario per permettere al lavoratore di godere dei benefici di legge (come ad esempio permessi o periodi prolungati di aspettativa con conservazione del posto di lavoro). Il datore di lavoro può anche venire a conoscenza dello stato di tossicodipendenza del dipendente, che richieda di accedere a programmi riabilitativi o terapeutici con conservazione del posto di lavoro.

Il datore di lavoro è legittimato a comunicare i dati idonei a rivelare lo stato di salute dei lavoratori ai soggetti pubblici (enti previdenziali e assistenziali) tenuti a erogare le prescritte indennità, in adempimento a specifici obblighi derivanti dalla legge, da altre norme o regolamenti o da previsioni contrattuali, nei limiti delle sole informazioni indispensabili.

informativa - Il datore di lavoro è tenuto a rendere al lavoratore, prima di procedere al trattamento dei dati personali che lo riguardano (anche in relazione alle ipotesi nelle quali la legge non richieda il suo consenso), un'informativa individualizzata completa degli elementi indicati dall'art. 13 del Codice.

misure di sicurezza - Il datore di lavoro deve adottare ogni misura di sicurezza, anche minima, prescritta dal Codice a protezione dei dati personali dei dipendenti, con particolare attenzione per quelli sensibili (art. 31 ss. e Allegato B). Le informazioni contenenti dati sensibili devono essere conservate separatamente da ogni altro dato personale dell'interessato, in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative.

Resta fermo l'obbligo del datore di lavoro di preporre alla custodia dei dati personali dei lavoratori apposito personale, specificamente incaricato del trattamento, che deve avere cognizioni in materia di protezione dei dati personali e ricevere una formazione adeguata. Secondo il Garante, in assenza di un'adeguata formazione degli addetti al trattamento dei dati personali, il rispetto della riservatezza dei lavoratori sul luogo di lavoro non potrà mai essere garantito.

Il datore di lavoro deve adottare misure organizzative e fisiche idonee a garantire:

- che i luoghi ove si svolge il trattamento dei dati siano protetti da indebite intrusioni;
- che sia evitata l'indebita presa di conoscenza dei dati da parte di terzi;
- che siano impartite istruzioni agli incaricati in ordine alla osservanza del segreto d'ufficio;
- che sia impedita l'acquisizione e riproduzione di dati personali trattati elettronicamente da parte di soggetti non autorizzati, in assenza di adeguati sistemi di autenticazione o autorizzazione;
- che sia impedita l'involontaria acquisizione di informazioni personali da parte di terzi o di altri dipendenti: ad esempio adottando opportuni accorgimenti per il rispetto di distanze di sicurezza o per la trattazione di informazioni riservate in spazi chiusi.

diritto di accesso - I lavoratori possono esercitare nei confronti del datore di lavoro i diritti previsti dall'art. 7 del Codice, tra cui il diritto di accedere ai dati che li riguardano, di ottenerne l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco se trattati in violazione di legge, di opporsi al trattamento per motivi legittimi.

La richiesta di accesso può riguardare anche informazioni di tipo valutativo.

Il datore di lavoro è tenuto a fornire un riscontro completo alla richiesta del lavoratore, comunicando in modo chiaro e intelligibile tutte le informazioni in suo possesso.

Il riscontro deve essere fornito nel termine di 15 giorni dal ricevimento dell'istanza del lavoratore; il termine è di 30 giorni, previa comunicazione all'interessato, se le operazioni sono di particolare complessità o se ricorre altro giustificato motivo (art. 146).

Il riscontro può essere fornito anche oralmente; in presenza di una specifica istanza, il datore di lavoro è tenuto a trasporre i dati su supporto cartaceo o informatico o a trasmetterli all'interessato per via telematica (art. 10).

Specie nei casi in cui è elevata la mole di informazioni personali detenute dal titolare del trattamento, il diritto di accesso può essere soddisfatto mettendo a disposizione dell'interessato il fascicolo personale, dal quale successivamente possono essere estratte le informazioni personali.

Nel fornire riscontro ad una richiesta di accesso, il titolare del trattamento deve comunicare i dati richiesti ed effettivamente detenuti, e non è tenuto a ricercare o raccogliere altri dati che non siano nella propria disponibilità e non siano oggetto, in alcuna forma, di attuale trattamento.

Il lavoratore può ottenere l'aggiornamento dei suoi dati personali.

L'eventuale rettifica dei dati personali indicati nel profilo professionale del lavoratore può avvenire solo in presenza della prova dell'effettiva e legittima attribuibilità delle qualifiche rivendicate dal lavoratore, che può comunque far valere in altra sede, sulla base di idoneo materiale probatorio, la propria pretesa al riconoscimento della qualifica o mansione rivendicata.

l'utilizzo della posta elettronica e di Internet nel rapporto di lavoro

Le linee guida per il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet[16], emanate dal Garante, richiamano il datore di lavoro ai principi di necessità, correttezza e pertinenza nel trattamento dei dati relativi alle navigazioni Internet e alle comunicazioni e-mail effettuate dai lavoratori, e forniscono concrete indicazioni in ordine all'uso del computer sul luogo di lavoro.

Il Garante prescrive ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli. Grava quindi sul datore di lavoro l'onere di:

- indicare chiaramente ed in modo particolareggiato le corrette modalità di utilizzo da parte dei lavoratori degli strumenti messi a disposizione;
- indicare le modalità e le finalità di eventuali controlli. Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive (ad esempio per rilevare anomalie o per manutenzioni) e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (art. 4, secondo comma, statuto dei lavoratori l. n. 300/1970); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Per uniformarsi a tale prescrizione il datore di lavoro sceglie la modalità informativa più consona a seconda del genere e della complessità delle attività svolte e della dimensione della struttura, e tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

Per le realtà aziendali complesse il Garante raccomanda l'adozione di un disciplinare interno[17], definito coinvolgendo anche le rappresentanze sindacali, nel quale ad esempio siano indicati:

- i comportamenti eventualmente non tollerati (ad esempio il download di software o di file musicali, o la tenuta di file privati nella rete interna);
- le modalità ed i tempi in cui sia eventualmente consentito l'utilizzo personale dei servizi di posta elettronica o di rete;
- le informazioni memorizzate temporaneamente (ad esempio le componenti di file di log eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- le informazioni eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di back up, della gestione tecnica della rete o di file di log);
- le modalità e le finalità di eventuali controlli (precisando ad esempio se, in caso di abusi singoli o reiterati, vengano inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);

[16] Provvedimento n. 13 del 1° marzo 2007, Gazzetta Ufficiale n. 58 del 10 marzo 2007 - doc. web n. 1387522

[17] Vedi il modello di disciplinare nel capitolo "i modelli"

- le conseguenze, anche di tipo disciplinare, che il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet siano utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di sua assenza programmata (ad esempio sistemi di risposta automatica dei messaggi ricevuti, contenente le “coordinate” di altri soggetti cui rivolgersi);
- l’eventuale possibilità di utilizzare i servizi per uso privato con pagamento a carico del lavoratore;
- le misure speciali per particolari realtà lavorative in cui i lavoratori siano tenuti al segreto professionale;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi, adottate ai sensi dell’Allegato B del Codice della privacy.

Oltre al disciplinare interno, alle realtà aziendali complesse è raccomandata l’adozione di misure organizzative e tecnologiche, consigliate nel provvedimento, volte a prevenire il rischio di utilizzi impropri.

Il Garante, infine, vieta a tutti i datori di lavoro di utilizzare sistemi hardware e software mirati ad effettuare il controllo a distanza dei lavoratori. Il divieto è stabilito dallo Statuto dei lavoratori (articolo 4, primo comma, Legge 300/1970), e l’eventuale trattamento dei dati acquisiti con tali installazioni è illecito, a prescindere dall’illiceità dell’installazione stessa. Ciò anche quando i singoli lavoratori ne siano consapevoli. Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art. 11, comma 2, del Codice della privacy). E’ quindi vietato:

- effettuare la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- riprodurre ed eventualmente memorizzare in modo sistematico le pagine web visualizzate dal lavoratore;
- leggere e registrare i caratteri inseriti tramite la tastiera o analogo dispositivo;
- effettuare l'analisi occulta di computer portatili affidati in uso.

Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad esempio per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelino necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentano indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinino un trattamento di dati personali riferiti o riferibili ai lavoratori. Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

l'attività promozionale e il contrasto allo spam

Il Garante ha varato le "Linee guida in materia di attività promozionale e contrasto allo spam"[18], finalizzate a combattere il marketing selvaggio e favorire pratiche commerciali "amiche" di utenti e consumatori.

Il provvedimento pone una particolare attenzione alle nuove frontiere dello spamming, quale quello diffuso sui social network (il cosiddetto social spam) o tramite alcune pratiche di "marketing virale" o "marketing mirato", che possono comportare modalità sempre più insidiose e invasive della sfera personale degli interessati.

Di seguito, i principi contenuti nelle Linee guida in materia di offerte commerciali e spam.

spam - Per poter inviare comunicazioni promozionali e materiale pubblicitario tramite sistemi automatizzati (telefonate preregistrate, e-mail, fax, sms, mms) è necessario aver prima acquisito il consenso dei destinatari (cosiddetto opt-in). Tale consenso deve essere specifico, libero, informato e documentato per iscritto.

Il consenso del destinatario è necessario per inviare messaggi promozionali agli utenti di Facebook, Twitter e altri social network (ad esempio pubblicandoli sulla loro bacheca virtuale) o di altri servizi di messaggistica e Voip sempre più diffusi come Skype, WhatsApp, Viber, Messenger, etc. Il fatto che i dati siano accessibili in rete non significa che possano essere liberamente usati per inviare comunicazioni promozionali automatizzate o per altre attività di marketing "virale" o "mirato".

Non è necessario il consenso per inviare e-mail o sms con offerte promozionali ad amici a titolo personale (il cosiddetto "passaparola").

soft spam – Il Garante consente il "soft spam" anche senza consenso, e cioè l'invio di messaggi promozionali, tramite e-mail, ai propri clienti su beni o servizi analoghi a quelli già acquistati. In tal caso si applica la deroga prevista dall'art. 130, comma 4, in base alla quale, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato. Ciò, però, sempre che si tratti di prodotti o servizi analoghi a quelli oggetto della vendita e che l'interessato, adeguatamente informato, non rifiuti tale uso.

promozioni per "fan" di marchi o aziende - Una impresa può inviare offerte commerciali ai propri "follower" sui social network quando dalla loro iscrizione alla pagina aziendale si evinca chiaramente l'interesse o il consenso a ricevere messaggi pubblicitari concernenti il marchio, il prodotto o il servizio offerto.

consenso unico per diverse attività di marketing - Il consenso prestato per l'invio di comunicazioni commerciali tramite modalità automatizzate (come e-mail o sms) copre anche quelle effettuate tramite posta cartacea o con telefonate tramite operatore.

[18] Provvedimento del 4 luglio 2013, pubblicato nella GU n. 174 del 26 luglio 2013 - doc. web n. 2542348

le sanzioni – Per l’omessa o inidonea informativa all'interessato, è applicabile la sanzione amministrativa da 6000 a 36000 euro, prevista dall’articolo 161. In caso di trattamento effettuato senza le previste misure di sicurezza, la sanzione amministrativa varia da 10000 a 120000 euro (articolo 162, comma 2 bis). Qualora il trattamento illecito assuma rilevanza di natura penale, potrebbe essere applicata la sanzione prevista dall'art. 167 del Codice (reclusione da 6 a 18 mesi).

la fidelizzazione dei clienti

Con uno specifico provvedimento[19] del 2005, il Garante ha stabilito le regole per i programmi di fidelizzazione, stabilendo alcuni principi necessari al fine di rendere i trattamenti di dati personali, raccolti attraverso tessere o carte di fidelizzazione, conformi alle norme vigenti.

principi generali - I sistemi e programmi informatici utilizzati per effettuare tali trattamenti devono essere configurati in modo da minimizzare l'utilizzo di informazioni relative a clienti identificabili. In applicazione del principio di necessità, viene considerato illecito il trattamento di dati della clientela se la profilazione può essere perseguita con dati anonimi.

Nel rispetto del principio di proporzionalità, tutti i dati personali devono essere pertinenti e non eccedenti rispetto alle finalità perseguite.

finalità della fidelizzazione – Possono essere trattati solo i dati necessari per attribuire i vantaggi connessi all'utilizzo della carta, e cioè:

- dati anagrafici dell'intestatario della carta;
- dati relativi al volume di spesa globale progressivamente realizzato, se necessari per l'attribuzione dei vantaggi medesimi e per il solo tempo a ciò strettamente necessario. L'eventuale conservazione di dati di dettaglio relativi alle particolari tipologie di beni o servizi acquistati, o di vantaggi conseguiti (punti, premi, bonus, ecc,) non è di regola considerata necessaria per la sola finalità di fidelizzazione; nei casi particolari in cui la conservazione è lecita, deve essere rispettato il principio di proporzionalità.

profilazione della clientela – L'attività di profilazione della clientela può essere svolta solo con dati anonimi e non identificativi, senza una relazione tra i dati che permetta di individuare il cliente e la sua sfera personale (gusti, preferenze, abitudini, bisogni e scelte di consumo).

Se la finalità può essere perseguita con tali modalità, non è lecito utilizzare e conservare dati personali o identificativi. Negli altri casi, le informazioni acquisite e le modalità del trattamento devono essere pertinenti e non eccedenti rispetto alla tipologia dei beni commercializzati o dei servizi resi.

Non è lecito utilizzare a fini di profilazione dati sensibili.

marketing diretto – E' consentito utilizzare i dati, pertinenti e non eccedenti, dei titolari della carta o dei suoi familiari, o di persone da essi indicate, per comunicazioni commerciali o per la vendita diretta, previo consenso differenziato dei diretti interessati.

[19] Provvedimento del 24 febbraio 2005 - doc. web n. 1103045

informativa – Prima del conferimento dei dati e del rilascio della carta deve essere fornita al cliente un'informativa chiara e completa, con modalità non suscettibili di incidere sulla libera scelta del cliente. Deve contenere tutti gli elementi richiesti dall'art. 13 del Codice, senza rimandare a "regolamenti di servizio", e deve essere agevolmente individuabile.

L'eventuale attività di profilazione e/o marketing deve essere posta in specifica evidenza, come pure l'intenzione di cedere a terzi specificamente individuati i dati per finalità da indicare puntualmente.

Deve risultare chiara la circostanza che, per gli scopi ulteriori, il conferimento dei dati ed il consenso sono liberi e facoltativi rispetto alla fidelizzazione in senso stretto.

adesione al programma di fidelizzazione e consenso al trattamento – Per ottenere la carta di fidelizzazione e fruire dei relativi vantaggi il cliente accetta condizioni contrattuali predisposte dall'emittente-titolare del trattamento. Il consenso del cliente al trattamento dei dati conferiti per la fidelizzazione non è quindi necessario, e pertanto non è corretto da parte dell'emittente sollecitare un inutile consenso.

E' invece necessario il consenso specifico, informato e differenziato, per ogni altra finalità del trattamento che comporti l'identificabilità degli interessati (profilazione e ricerche di mercato, marketing). L'adesione all'iniziativa di fidelizzazione non può essere condizionata alla manifestazione di tale consenso.

Non è lecito raccogliere un consenso generale, comprendendo anche i casi in cui il consenso non è necessario, o a prescindere dalle finalità perseguite.

Per le comunicazioni in forma elettronica o sistemi automatizzati occorre uno specifico consenso.

conservazione dei dati – I titolari del trattamento devono individuare termini massimi di conservazione dei dati, tenendo conto del fatto che i dati non necessari agli scopi per i quali sono trattati vanno cancellati o trasformati in forma anonima.

In ogni caso i dati relativi al dettaglio degli acquisti relativi a clienti individuabili possono essere conservati per finalità di profilazione o marketing per un periodo non superiore rispettivamente a 12 o 24 mesi.

In caso di ritiro, disabilitazione per mancato utilizzo, scadenza o restituzione della carta, deve essere individuato un termine di conservazione dei dati personali a soli fini amministrativi non superiore a 3 mesi

altri obblighi - Restano ovviamente fermi gli altri obblighi imposti dal Codice:

- notificazione al Garante, se si effettuano trattamenti con l'ausilio di strumenti elettronici volti a definire profili di consumatori e ad analizzare abitudini e scelte in ordine ai prodotti o servizi acquistati;
- adozione delle misure minime di sicurezza;
- individuazione degli incaricati;
- adozione di idonee misure per l'esercizio dei diritti degli interessati.

la profilazione dei clienti da parte delle strutture ricettive

Il Garante della privacy, nel corso di accertamenti effettuati in ambiti alberghieri[20], ha rilevato, in alcuni casi e per alcuni trattamenti, la non conformità alle prescrizioni del Codice.

Le ispezioni hanno riguardato i seguenti diversi trattamenti (rispetto a quelli obbligatori per legge ed a quelli indispensabili per dar corso al contratto d'albergo) da parte di aziende alberghiere:

- definizione dei profili dei clienti;
- attuazione di operazioni a premio, attraverso apposito programma;
- svolgimento di attività di marketing, limitata ai clienti aderenti al programma di operazione a premio;
- trattamento di dati personali riferiti a soggetti iscritti on-line alla newsletter della società.

Nelle considerazioni pubblicate a seguito delle ispezioni, il Garante ha rinviato ai principi contenuti nel provvedimento generale sulle "Fidelity card"[21], nel quale si evidenzia la necessità che il cliente sia preventivamente informato sull'uso dei suoi dati, ed esprima uno specifico consenso. Anche nel settore ricettivo, nell'ambito dei programmi di fidelizzazione, i dati relativi ai gusti, abitudini, durata dei pernottamenti, ed ogni altra informazione utile per conoscere meglio il cliente e anticiparne le richieste, possono essere raccolti e rielaborati solo rispettando le prescrizioni del Codice.

principio di necessità e pertinenza – I sistemi e i programmi informatici utilizzati per effettuare tali trattamenti devono essere configurati in modo da minimizzare l'utilizzo di informazioni relative a clienti identificabili. In applicazione del principio di necessità, viene considerato illecito il trattamento di dati della clientela se la profilazione può essere perseguita con dati anonimi.

Nel rispetto del principio di pertinenza e proporzionalità, il Garante ha segnalato la necessità che siano identificati tempi massimi di conservazione dei dati alla luce delle finalità in concreto perseguite. In particolare, per le seguenti operazioni il Garante ha indicato i tempi congrui:

- realizzazione delle operazioni a premio - possono essere conservati i dati relativi al solo ammontare degli esborsi effettuati sino al conseguimento da parte del cliente del vantaggio previsto, e comunque non oltre la scadenza del termine dell'operazione a premio indicata nel relativo regolamento;
- creazione dei profili dei clienti - risulta congrua la conservazione dei dati per 12 mesi decorrenti dalla registrazione delle informazioni.

informativa – Nel caso in cui vi siano diverse modalità di raccolta delle informazioni della clientela – in occasione del soggiorno in albergo, con l'adesione all'operazione a

[20] Provvedimento 9 marzo 2006, doc. web n. 1252220 e provvedimento 31 gennaio 2008, doc web n. 1490553

[21] Provvedimento del 24 febbraio 2005 - doc. web n. 1103045

premio, mediante la compilazione di modelli resi disponibili on-line – in ciascuna circostanza, e indipendentemente dal mezzo di volta in volta utilizzato, debbono essere rese le informazioni sul trattamento previste dal Codice.

consenso al trattamento – Il Garante ha ricordato la necessità di acquisire uno specifico ed informato consenso dell'interessato nel caso di trattamento per ulteriori finalità di marketing o di definizione dei profili dei clienti. Il consenso non è invece necessario con riguardo ai dati trattati in base ad obblighi di legge (ad esempio per assolvere ad obblighi contabili e tributari o all'obbligo previsto dall'art. 109 TULPS). Non occorre inoltre il consenso per le operazioni di trattamento finalizzate all'esecuzione del contratto – ivi comprese quelle derivanti dall'operazione a premio - o per adempiere, anche in fase precontrattuale, a specifiche richieste del cliente.

Devono invece essere individuate specifiche modalità che consentano ai clienti di esprimere liberamente e specificamente, anche nei modelli on−line, le proprie scelte in ordine allo svolgimento da parte dell'albergo di attività di marketing, trattandosi di una finalità differente da quella concernente la prestazione alberghiera.

Gli interessati devono essere messi in grado di esprimere consapevolmente e liberamente le proprie scelte in ordine al trattamento dei loro dati, manifestando il proprio consenso per ciascuna diversa finalità perseguita dal titolare del trattamento.

Nel caso di prenotazione on line, i moduli di acquisizione dei dati presenti nel sito web dell'albergo devono infatti consentire al cliente di esprimere un consenso libero e specifico al trattamento dei dati a scopo commerciale, rendendo possibile l'acquisizione di un consenso specifico per il suo perseguimento (ad esempio, predisponendo un distinto check box per chi, oltre a richiedere il servizio, intenda autorizzare il titolare del trattamento allo svolgimento di tale attività).

notificazione dei trattamenti per finalità di definizione dei profili della clientela – Ai sensi del Codice sulla privacy, nel caso in cui le operazioni di trattamento, effettuate con l'ausilio di strumenti elettronici, siano finalizzate ad analizzare preferenze e scelte di consumo degli interessati, occorre effettuare la notificazione al Garante.

la videosorveglianza

Con un provvedimento dell'8 aprile 2010[22], che sostituisce un precedente provvedimento del 2004[23], il Garante per la privacy ha emanato alcune disposizioni in materia di videosorveglianza.

La prima parte del provvedimento richiama alcuni principi generali ed illustra le prescrizioni applicabili a tutti i sistemi di videosorveglianza. La seconda parte illustra invece le prescrizioni riguardanti specifici trattamenti di dati. Per casi particolari, l'Autorità si riserva di intervenire di volta in volta con atti ad hoc.

impiego di strumenti di sorveglianza senza consenso degli interessati – Nell'ambito del principio del "bilanciamento degli interessi", il provvedimento stabilisce che la rilevazione delle immagini può avvenire senza consenso degli interessati quando sia effettuata per perseguire un legittimo interesse del titolare o per fini di tutela delle persone e dei beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo o per finalità di prevenzione incendi o di sicurezza del lavoro.

La videosorveglianza è quindi ammessa in presenza di concrete situazioni che la giustifichino, a protezione delle persone, della proprietà o del patrimonio aziendale.

oggetto delle riprese - Nell'uso delle apparecchiature volte a riprendere, con o senza registrazione delle immagini, aree esterne ad edifici e immobili (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza) il trattamento deve essere effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti e di particolari non rilevanti (per esempio, vie, esercizi commerciali, edifici, etc.).

informativa - Il Garante conferma che gli interessati devono essere sempre informati che stanno per accedere ad una zona videosorvegliata. A tal fine, può essere utilizzato un cartello con informazioni minime, riportante il nome del titolare del trattamento e la finalità perseguita. Tale cartello:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

Il Garante ritiene auspicabile che l'informativa, se resa in forma semplificata (anche avvalendosi del modello di cui all'allegato 1 alla delibera in oggetto), sia disponibile in un testo completo con modalità facilmente accessibili e anche con strumenti informatici e

[22] Provvedimento dell'8 aprile 2010, GU n. 99 del 29 aprile 2010 - doc. web n. 1712680

[23] Provvedimento del 29 aprile 2004 – doc. web n.1003482

telematici (in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, messaggi preregistrati disponibili digitando un numero telefonico gratuito).

In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice.

Deve inoltre essere resa nota agli interessati la circostanza che il sistema di videosorveglianza sia collegato direttamente con le forze di polizia, utilizzando eventualmente il modello semplificato di cui all'allegato 2 della delibera.

verifica preliminare - I trattamenti effettuati dalle imprese ricettive non richiedono, nella generalità dei casi, una verifica preliminare da parte del Garante. La verifica preliminare è infatti necessaria quando vi è l'associazione delle immagini a dati biometrici o l'uso di sistemi "intelligenti" in grado di rilevare automaticamente comportamenti o eventi anomali. Va invece posta particolare attenzione a non eccedere i tempi massimi di conservazione delle immagini registrate per non ricadere nell'obbligo di richiedere all'Autorità una verifica preliminare.

misure di sicurezza - Come regola generale, i dati raccolti mediante la videosorveglianza devono essere protetti per ridurre al minimo i rischi di distruzione, perdita accidentale, accessi non autorizzati o trattamenti non consentiti. E' pertanto fortemente consigliabile che, specie nelle aziende di minori dimensioni, alle immagini acceda unicamente il titolare al fine di evitare l'individuazione di specifiche figure autorizzate e l'adozione di misure organizzative per verificarne l'attività. All'aumentare della dimensione aziendale, viceversa, dovranno essere adottati:

- diversi livelli di visibilità e trattamento delle immagini (designazione per iscritto di un numero delimitato di incaricati ad accedere ai locali dove sono situate le postazioni di controllo, ad utilizzare gli impianti e, nei casi in cui ciò sia indispensabile, a visionare le immagini; individuazione dei diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore distinguendo tra chi è unicamente abilitato a visionare le immagini da chi può effettuare ulteriori operazioni) anche attraverso l'attribuzione di credenziali di autenticazione che abilitino ad effettuare unicamente le operazioni di propria competenza;
- accorgimenti per limitare la possibilità, per i soggetti abilitati, di visionare le immagini registrate e di effettuare sulle stesse operazioni di cancellazione e duplicazione;
- accorgimenti per garantire la cancellazione anche automatica delle registrazioni dopo 24 ore dalla rilevazione. Solo in alcuni casi (come i mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (il Provvedimento cita come esempio le banche ma si ritiene che possano essere ricomprese anche altre attività come le gioiellerie) può ritenersi ammesso un periodo più lungo comunque non eccedente la settimana;
- accorgimenti per garantire, nel caso di interventi di manutenzione, che i soggetti a ciò preposti possano accedere alle immagini soltanto se questo si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti abilitati alla visione delle immagini;
- accorgimenti contro il rischio di accesso abusivo alle reti informatiche nel caso di apparati digitali connessi a reti informatiche;

- accorgimenti per l'applicazione di tecniche crittografiche nel caso di trasmissione tramite una rete pubblica di comunicazioni.

durata della eventuale conservazione delle immagini - La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura dell'esercizio, nonché nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, il Garante ritiene non debba comunque superare la settimana.

Un eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e deve comunque essere preventivamente sottoposto alla verifica del Garante.

sistemi integrati di videosorveglianza – Sono i sistemi che offrono servizi centralizzati di videosorveglianza remota da parte di vari soggetti (società di vigilanza, Internet e service providers, fornitori di video specialistici, ecc.) oltre alle forze di polizia.

Questi diversi sistemi possono prevedere:

- la gestione coordinata dei servizi di videosorveglianza tramite condivisione delle immagini da parte di diversi e autonomi titolari del trattamento che utilizzano le medesime infrastrutture tecnologiche. In tal caso ciascun titolare può trattare le immagini strettamente funzionali al perseguimento delle finalità dichiarate nell'informativa;
- il collegamento telematico di diversi titolari ad un centro unico gestito da un terzo. Tale soggetto terzo va designato responsabile da parte di ogni singolo titolare e deve assumere un ruolo di coordinamento e gestione dell'attività di videosorveglianza senza consentire forme di correlazione delle immagini raccolte per conto di ciascun titolare;
- il collegamento con le sale o le centrali operative degli organi di polizia.

Per tali sistemi:

1. devono essere adottati sistemi per la registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate con conservazione non inferiore a sei mesi;
2. deve essere predisposta una separazione logica delle immagini registrate dai diversi titolari.

Nel caso in cui le misure sopra riportate non siano integralmente applicabili per la natura e le caratteristiche dei sistemi di videosorveglianza utilizzati, il titolare è tenuto a richiedere una verifica preventiva all'Autorità.

rapporti di lavoro – Il provvedimento conferma il divieto di controllo a distanza dell'attività lavorativa nell'uso di sistemi di videosorveglianza stabilito nello Statuto dei

lavoratori. È vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge). Vanno poi osservate le garanzie previste dallo Statuto dei lavoratori quando la videosorveglianza è resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro: in tali casi, ai sensi dell'art. 4 della l. n. 300/1970, occorre il preventivo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.

Tali garanzie vanno osservate sia all'interno degli edifici, sia in altri contesti in cui è resa la prestazione di lavoro.

Sotto un diverso profilo, eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice Privacy, fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi, per motivi legittimi, alla sua diffusione.

utilizzo di web cam a scopi promozionali-turistici o pubblicitari - Le attività di rilevazione di immagini a fini promozionali-turistici o pubblicitari, attraverso web cam, devono avvenire con modalità che rendano non identificabili i soggetti ripresi. Ciò in considerazione del concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete Internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle predette finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento.

le sanzioni – Le sanzioni applicabili sono le seguenti:

- violazione delle disposizioni riguardanti l'informativa (es. mancata indicazione del titolare, della finalità perseguita e dell'eventuale collegamento con le forze di polizia) - sanzione amministrativa da 6000 a 36000 euro (art. 161)
- mancato rispetto delle specifiche prescrizioni del provvedimento - sanzione amministrativa da 30000 a 180000 euro (art. 162, comma 2-ter)
- omessa adozione delle generiche misure minime di sicurezza - sanzione amministrativa da 10000 a 120000 euro (art. 162, comma 2-bis) ed eventuale sanzione penale prevista dall'art. 169 (arresto sino a due anni)
- mancato rispetto dei tempi di conservazione delle immagini raccolte e del correlato obbligo di cancellazione di dette immagini oltre il termine previsto - sanzione amministrativa da 30000 a 180000 euro (art. 162, comma 2-ter)
- utilizzo di sistemi di videosorveglianza preordinati al controllo a distanza dei lavoratori o ad effettuare indagini sulle loro opinioni - ammenda da euro 154 a euro 1.549 o arresto da 15 giorni ad un anno (art. 171 del Codice; art. 38 Statuto dei lavoratori)

l'uso dei cookie

Il Garante, con un provvedimento[24] adottato al termine di una consultazione pubblica, ha regolamentato l'installazione dei cookie per finalità di profilazione e marketing da parte dei gestori dei siti web.

I cookie sono piccoli file di testo che i siti visitati inviano al terminale (computer, tablet, smartphone, notebook) dell'utente, dove vengono memorizzati, per poi essere ritrasmessi agli stessi siti alla visita successiva. Sono usati per eseguire autenticazioni informatiche, monitoraggio di sessioni e memorizzazione di informazioni sui siti (senza l'uso dei cookie "tecnici" alcune operazioni risulterebbero molto complesse o impossibili da eseguire). Ma attraverso i cookie si può anche monitorare la navigazione, raccogliere dati su gusti, abitudini, scelte personali che consentono la ricostruzione di dettagliati profili dei consumatori.

Al fine di giungere a una corretta regolamentazione di tali dispositivi, è necessario distinguerli sulla base delle finalità perseguite da chi li utilizza. Infatti l'obbligo di acquisire il consenso preventivo e informato degli utenti è previsto solo in caso di installazione di cookie utilizzati per finalità diverse da quelle meramente tecniche.

Si individuano pertanto due macro-categorie: cookie "tecnici" e cookie "di profilazione".

cookie tecnici - I cookie tecnici sono quelli utilizzati al solo fine di "effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio". Essi non vengono utilizzati per scopi ulteriori e sono normalmente installati direttamente dal titolare o gestore del sito web. Possono essere suddivisi in:

- cookie di navigazione o di sessione, che garantiscono la normale navigazione e fruizione del sito web (permettendo, ad esempio, di realizzare un acquisto o autenticarsi per accedere ad aree riservate);
- cookie analytics, assimilati ai cookie tecnici laddove utilizzati direttamente dal gestore del sito per raccogliere informazioni, in forma aggregata, sul numero degli utenti e su come questi visitano il sito stesso;
- cookie di funzionalità, che permettono all'utente la navigazione in funzione di una serie di criteri selezionati (ad esempio, la lingua, i prodotti selezionati per l'acquisto) al fine di migliorare il servizio reso allo stesso.

Per l’uso di tali cookie non è richiesto il preventivo consenso degli utenti, mentre resta fermo l'obbligo di dare l'informativa[25] ai sensi dell'art. 13 del Codice, che il gestore del sito potrà fornire con le modalità che ritiene più idonee. L'uso dei cookie tecnici è sottratto all'obbligo di notificazione al Garante di cui all’articolo 37 del Codice.

[24] Provvedimento del 8 maggio 2014, GU n. 126 del 3 giugno 2014 - doc. web n. 3118884

[25] Vedi il modello di informativa per il sito web nel capitolo “i modelli”

cookie di profilazione - I cookie di profilazione sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete. In ragione della particolare invasività che tali dispositivi possono avere nell'ambito della sfera privata degli utenti, la normativa europea e italiana prevede che l'utente debba essere adeguatamente informato sull'uso degli stessi ed esprimere così il proprio valido consenso.

L'uso dei cookie ai fini di profilazione rientra tra i trattamenti soggetti all'obbligo di notificazione al Garante ai sensi dell'art. 37, comma 1, lett. d), del Codice.

Nel caso di uso di cookie di profilazione, per proteggere la privacy dei utenti che navigano sui siti e consentire loro scelte più consapevoli, il Garante ha dunque stabilito che, quando si accede alla home page o ad un'altra pagina di un sito web deve immediatamente comparire un banner ben visibile, in cui sia indicato chiaramente:

- che il sito utilizza cookie di profilazione per inviare messaggi pubblicitari mirati;
- che il sito consente anche l'invio di cookie di "terze parti", ossia di cookie installati da un sito diverso tramite il sito che si sta visitando;
- un link a una informativa più ampia, con le indicazioni sull'uso dei cookie inviati dal sito, dove è possibile negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei cookie di "terze parti";
- l'indicazione che proseguendo nella navigazione (ad es., accedendo ad un'altra area del sito o selezionando un'immagine o un link) si presta il consenso all'uso dei cookie.

Per quanto riguarda l'obbligo di tener traccia del consenso dell'utente, al gestore del sito è consentito utilizzare un cookie tecnico, in modo tale da non riproporre l'informativa breve alla seconda visita dell'utente.

L'utente mantiene, comunque, la possibilità di modificare le proprie scelte sui cookie attraverso l'informativa estesa, che deve essere linkabile da ogni pagina del sito.

ANALISI DEI TRATTAMENTI TIPICI DELLE AZIENDE RICETTIVE

la prenotazione

La prenotazione di un soggiorno presso una struttura ricettiva, sia che avvenga telefonicamente, per iscritto o tramite Internet o posta elettronica, implica necessariamente il trattamento da parte dell'azienda dei dati personali (nome e cognome, indirizzo, numero di telefono, eventualmente estremi della carta di credito, eccetera) di colui che effettua la prenotazione, o di coloro per i quali il soggiorno è prenotato.

Per tale trattamento il titolare, e cioè l'azienda ricettiva, è tenuto ai seguenti adempimenti:

l'informativa - All'atto della conferma della prenotazione, va data una corretta informativa all'interessato. L'informativa può essere data oralmente o per iscritto.

il consenso – Non è necessario acquisire il consenso dell'interessato, trattandosi di un trattamento effettuato nell'ambito dei normali adempimenti precontrattuali. E' invece necessario acquisire il consenso scritto dell'interessato, nel caso, non rarissimo, in cui oltre ai normali dati personali vengano conferiti anche dati sensibili (ad esempio, nel caso di richieste particolari che possano far desumere una malattia o un handicap, la religione professata, l'appartenenza ad un gruppo politico o ad un sindacato, eccetera).

la notificazione al Garante – Per tali trattamenti non va effettuata la notificazione al Garante.

l'autorizzazione del Garante – Con l'autorizzazione generale n. 5/2014 sono stati autorizzati i trattamenti di dati sensibili, fatta eccezione per quelli idonei a rivelare la vita sessuale, effettuati da parte delle imprese che operano nel settore turistico o alberghiero.

le modalità di raccolta ed i requisiti dei dati – I dati vanno trattati in modo lecito e con correttezza e con le altre cautele previste dall'articolo 11 del Codice.

le misure di sicurezza – Vanno adottate le misure di sicurezza di cui agli articoli da 33 a 36 del Codice, specificate nel disciplinare tecnico contenuto nell'allegato B. Le misure minime di sicurezza da adottare vanno differenziate a seconda delle modalità con cui viene effettuato il trattamento e del tipo di dati (sensibili o non sensibili).

la registrazione a fini di polizia

L'articolo 109 del Testo Unico delle leggi di pubblica sicurezza[26] stabilisce che i gestori di strutture ricettive non possono dare alloggio a persone sfornite di documento di riconoscimento. Inoltre, i gestori comunicano alle questure, avvalendosi di mezzi informatici o telematici o mediante fax, le generalità delle persone alloggiate, secondo modalità stabilite con decreto ministeriale[27].

Per tale trattamento l'azienda ricettiva è tenuta ai seguenti adempimenti:

l'informativa - All'atto dell'acquisizione delle generalità, va data al cliente una corretta informativa. L'informativa può essere data oralmente o per iscritto, eventualmente utilizzando un cartello da affiggere alla reception della struttura[28].

il consenso – Non è necessario acquisire il consenso del cliente, trattandosi di un trattamento effettuato in base ad un obbligo di legge, ed inoltre i dati trattati non sono sensibili.

la notificazione al Garante – Per tali trattamenti la notificazione al Garante non va effettuata.

l'autorizzazione del Garante – Non è necessaria, dal momento che i dati trattati non sono sensibili.

le modalità di raccolta ed i requisiti dei dati – I dati vanno trattati in modo lecito e con correttezza e con le altre cautele previste nell'articolo 11 del Codice.

le misure di sicurezza – Vanno adottate le misure di sicurezza individuate negli articoli da 33 a 36 del Codice e nel disciplinare tecnico contenuto nell'allegato B. Le misure minime di sicurezza da adottare vanno differenziate a seconda delle modalità con cui viene effettuato il trattamento.

[26] Approvato con RD 18 giugno 1931, n.773.

[27] Decreto del Ministero dell'Interno 7 gennaio 2013 "Disposizioni concernenti la comunicazione alle autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive".

[28] Vedi il modello di informativa al cliente riportato nel capitolo "i modelli"

il servizio di ricevimento e portineria

Per i trattamenti che comportano la comunicazione esterna di dati relativi al soggiorno dei clienti, effettuati nell'ambito del servizio di ricevimento di messaggi e telefonate, il titolare del trattamento è tenuto ai seguenti adempimenti:

l'informativa - All'atto dell'acquisizione dei dati, va data una corretta informativa all'interessato. L'informativa può essere data oralmente o per iscritto[29].

il consenso – Secondo il Garante, è necessario acquisire il consenso dell'interessato[30].

la notificazione al Garante – Per tali trattamenti, la notificazione al Garante non va effettuata.

l'autorizzazione del Garante – Non è necessaria, dal momento che i dati trattati non sono sensibili. Nel caso eventuale di acquisizione di dati sensibili, l'autorizzazione generale n. 5/2014 autorizza i trattamenti di dati sensibili, fatta eccezione per quelli idonei a rivelare la vita sessuale, effettuati da parte delle imprese che operano nel settore turistico o alberghiero.

le modalità di raccolta ed i requisiti dei dati – I dati vanno trattati in modo lecito e con correttezza e con le altre cautele previste nell'articolo 11 del Codice.

le misure di sicurezza – Vanno adottate le misure di sicurezza individuate negli articoli da 33 a 36 del Codice e nel disciplinare tecnico contenuto nell'allegato B. Le misure minime di sicurezza da adottare vanno differenziate a seconda delle modalità con cui viene effettuato il trattamento.

[29] Vedi il modello di informativa al cliente riportato nel capitolo "i modelli"

[30] Vedi il modello di acquisizione del consenso del cliente nel capitolo "i modelli"

le iniziative promozionali e pubblicitarie

Molto spesso le aziende ricettive conservano i dati dei clienti, acquisiti nel momento della prenotazione o al momento dell'arrivo, e li utilizzano per inviare periodicamente gli aggiornamenti delle proprie tariffe, pubblicizzare offerte speciali, o semplicemente inviare gli auguri per il compleanno o per le festività, sempre comunque con fine promozionale. Per tali trattamenti l'azienda ricettiva è tenuta ai seguenti adempimenti:

l'informativa - All'atto dell'acquisizione dei dati va data una corretta informativa all'interessato. L'informativa può essere data oralmente o per iscritto[31].

il consenso – E' necessario acquisire il consenso dell'interessato[32].

la notificazione al Garante – Per tali trattamenti la notificazione al Garante non va effettuata.

l'autorizzazione del Garante – Non è necessaria, dal momento che i dati trattati non sono sensibili.

le modalità di raccolta ed i requisiti dei dati – I dati vanno trattati in modo lecito e con correttezza e con le altre cautele previste nell'articolo 11 del Codice.

le misure di sicurezza – Vanno adottate le misure di sicurezza individuate negli articoli da 33 a 36 del Codice e nel disciplinare tecnico contenuto nell'allegato B. Le misure minime di sicurezza da adottare vanno differenziate a seconda delle modalità con cui viene effettuato il trattamento.

[31] Vedi il modello di informativa al cliente riportato nel capitolo "i modelli"

[32] Vedi il modello di acquisizione del consenso del cliente nel capitolo "i modelli"

i programmi di fidelizzazione dei clienti

Per i trattamenti dei dati dei clienti nell'ambito dei programmi di fidelizzazione, attraverso il rilascio di tessere o carte, finalizzati ad attribuire vantaggi ai possessori delle stesse, l'azienda ricettiva è tenuta ai seguenti adempimenti:

l'informativa - All'atto dell'acquisizione dei dati va data una corretta informativa all'interessato.

il consenso – Non va richiesto il consenso dei clienti per l'uso dei loro dati finalizzato al rilascio di carte di fedeltà ai soli fini di sconti, premi, bonus, servizi accessori, facilitazioni di pagamento. E' necessario acquisire il consenso libero ed informato dei clienti quando i dati personali raccolti tramite la carte di fedeltà vengono usati anche ad altri fini, quali, ad esempio, il marketing personalizzato, lo studio dei comportamenti e delle scelte d'acquisto, l'individuazione di fasce di reddito. I clienti hanno diritto di non dare il consenso all'uso dei dati per tali scopi, senza per questo dover rinunciare alla carta di fidelizzazione.

la notificazione al Garante – L'obbligo di notificazione al Garante sussiste nel caso di trattamenti, effettuati mediante l'ausilio di strumenti elettronici, volti a definire profili di consumatori o ad analizzarne abitudini e scelte in ordine ai prodotti acquistati.

l'autorizzazione del Garante – Non è necessaria, sempreché non vengano trattati dati sensibili.

le modalità di raccolta ed i requisiti dei dati – I dati vanno trattati in modo lecito e con correttezza e con le altre cautele previste nell'articolo 11 del Codice.

le misure di sicurezza – Vanno adottate le misure di sicurezza individuate negli articoli da 33 a 36 del Codice e nel disciplinare tecnico contenuto nell'allegato B. Le misure minime di sicurezza da adottare vanno differenziate a seconda delle modalità con cui viene effettuato il trattamento.

trattamento dei dati relativi ai lavoratori

Per i trattamenti di dati personali relativi a coloro che lavorano in azienda, il titolare è tenuto ai seguenti adempimenti:

l'informativa - All'atto dell'acquisizione dei dati, va data una corretta informativa all'interessato. L'informativa può essere data oralmente o per iscritto[33].

il consenso – E' necessario acquisire il consenso scritto del lavoratore, dal momento che il trattamento può riguardare anche dati sensibili (dati idonei a rivelare lo stato di salute o le convinzioni politiche, o religiose, o l'adesione a sindacati, eccetera)[34].

la notificazione al Garante – Per tali trattamenti, la notificazione al Garante non va effettuata.

l'autorizzazione del Garante – Con l'autorizzazione generale n. 1/2014, il Garante ha legittimato il trattamento di dati sensibili finalizzato alla gestione dei rapporti di lavoro.

le modalità di raccolta ed i requisiti dei dati – I dati vanno trattati in modo lecito e con correttezza e con le altre cautele previste nell'articolo 11 del Codice.

le misure di sicurezza – Vanno adottate le misure di sicurezza individuate negli articoli da 33 a 36 del Codice e nel disciplinare tecnico contenuto nell'allegato B. Le misure minime di sicurezza da adottare vanno differenziate a seconda delle modalità con cui viene effettuato il trattamento e del tipo di dati, sensibili o non sensibili.

[33] Vedi il modello di informativa ai lavoratori riportato nel capitolo "i modelli"

[34] Vedi il modello di acquisizione del consenso del lavoratore nel capitolo "i modelli"

trattamento dei dati relativi ai fornitori

Per i trattamenti di dati personali relativi ai fornitori di beni e servizi, il titolare è tenuto ai seguenti adempimenti:

l'informativa - All'atto dell'acquisizione dei dati, va data una corretta informativa all'interessato. L'informativa può essere data oralmente o per iscritto.

il consenso – Non è necessario acquisire il consenso del fornitore.

la notificazione al Garante – Per tali trattamenti, il Codice non prevede l'obbligo di effettuare la notificazione al Garante.

l'autorizzazione del Garante – Non è necessaria, dal momento che i dati trattati non sono sensibili.

le modalità di raccolta ed i requisiti dei dati – I dati vanno trattati in modo lecito e con correttezza e con le altre cautele previste nell'articolo 11 del Codice.

le misure di sicurezza – Vanno adottate le misure di sicurezza individuate negli articoli da 33 a 36 del Codice e nel disciplinare tecnico contenuto nell'allegato B. Le misure minime di sicurezza da adottare vanno differenziate a seconda delle modalità con cui viene effettuato il trattamento.

I MODELLI

l’articolo 7

Il testo dell’articolo 7 del Codice sulla privacy deve essere sempre tenuto a disposizione di coloro i cui dati sono oggetto di trattamento:

Articolo 7. Diritto di accesso ai dati personali ed altri diritti.

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

l'informativa al cliente

Il modello che segue, modificato e integrato a seconda delle specifiche esigenze, va fatto visionare all'arrivo del cliente o può essere affisso al ricevimento.

Gentile Cliente,

desideriamo informarla, ai sensi dell'articolo 13 del Codice sulla privacy (D. Legisl. 196/2003), che il trattamento dei suoi dati personali avverrà con correttezza e trasparenza, per fini leciti e tutelando la sua riservatezza ed i suoi diritti.

Il trattamento sarà effettuato anche con l'ausilio di mezzi informatici per le seguenti finalità:

1. per adempiere all'obbligo previsto dall'articolo 109 del R.D. 18.6.1931 n. 773, che ci impone di comunicare alla Questura le generalità dei clienti alloggiati;
2. per adempiere ai vigenti obblighi amministrativi, contabili e fiscali;
3. per espletare la funzione di ricevimento di messaggi e telefonate a lei indirizzati;
4. per accelerare le procedure di registrazione in caso di suoi successivi soggiorni presso il nostro albergo. Per tale finalità i suoi dati saranno conservati per il periodo massimo di ……;
5. per inviarle nostri messaggi promozionali e aggiornamenti sulle tariffe e sulle offerte praticate.

Desideriamo inoltre informarla che il conferimento dei suoi dati per i trattamenti di cui ai punti 1 e 2 è obbligatorio, ed in caso di rifiuto a fornirli non potremo ospitarla nella nostra struttura.

Se desidera che siano effettuati i trattamenti di cui ai punti 3, 4 e 5 dovrà invece fornirci il suo consenso. Il consenso potrà comunque essere successivamente revocato opponendosi ai trattamenti.

Per qualsiasi ulteriore informazione, e per far valere i diritti a lei riconosciuti dall'articolo 7 del Codice sulla privacy (D. Legisl. 196/2003), potrà rivolgersi al Titolare / Responsabile dei trattamenti ……

l'acquisizione del consenso del cliente

Il modello, integrato e modificato secondo le specifiche esigenze, può essere fatto sottoscrivere al cliente all'arrivo presso la struttura ricettiva.

Io sottoscritto …… ai sensi del Codice sulla privacy (D. Legisl. 196/2003), ricevuta l'informativa sul trattamento dei miei dati personali:

- *autorizzo / non autorizzo la struttura ricettiva alla comunicazione esterna di dati relativi al mio soggiorno al fine esclusivo di consentire la funzione di ricevimento di messaggi e telefonate a me indirizzati*
- *autorizzo / non autorizzo la struttura ricettiva alla conservazione delle mie generalità al fine di accelerare le procedure di registrazione in caso di miei successivi soggiorni*
- *autorizzo / non autorizzo la struttura ricettiva ad inviare al mio domicilio o al mio indirizzo di posta elettronica periodica documentazione sulle tariffe e sulle offerte praticate.*

Data e firma ……..

l'informativa sul sito web

Riportiamo di seguito un modello di "privacy policy" da inserire nel sito web della struttura ricettiva. Il testo va modificato ed integrato in relazione agli ambiti di operatività ed alle funzioni effettivamente svolte.

la privacy policy di questo sito

In questa pagina si descrivono le modalità di gestione del sito in riferimento al trattamento dei dati personali degli utenti che lo consultano. Si tratta di un'informativa che è resa anche ai sensi dell'art. 13 del decreto legislativo n. 196/2003 - Codice in materia di protezione dei dati personali - a coloro che consultano le pagine del sito internet www. …….. (di seguito: "sito") o che usufruiscono dei servizi sullo stesso messi a disposizione.

L'informativa è resa esclusivamente per il sito di ……e non anche per gli altri siti web eventualmente consultati dall'utente tramite i link presenti all'interno del sito.

titolare del trattamento

Titolare del trattamento è ……., con sede in ……. Via…… (indicare anche l'eventuale Responsabile)

tipi di dati trattati

dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento di questo sito web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito: salva questa eventualità, allo stato i dati sui contatti web non persistono per più di sette giorni[35]*.*

Dati forniti volontariamente dall'utente

[35] Indicare gli effettivi giorni di permanenza dei dati.

La registrazione dei dati personali, anche sensibili, sulla apposita pagina del sito, finalizzata a richiedere servizi, l'accesso alle aree riservate del Sito, l'invio della newsletter, nonché l'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati su questo sito, comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti.

Specifiche informative di sintesi verranno progressivamente riportate o visualizzate nelle pagine del sito predisposte per particolari servizi a richiesta.

Cookie[36]

Nessun dato personale degli utenti viene in proposito acquisito dal sito.

Non viene fatto uso di cookie per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookie persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

L'uso di c.d. cookie di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del sito.

I c.d. cookie di sessione utilizzati in questo sito evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

Facoltatività del conferimento dei dati

A parte quanto specificato per i dati di navigazione, l'utente è libero di fornire i dati personali riportati nei moduli di richiesta di servizi, o comunque indicati in contatti con i nostri uffici per sollecitare l'invio della newsletter, di materiale informativo o di altre comunicazioni.

Il loro mancato conferimento può comportare l'impossibilità di ottenere quanto richiesto.

Modalità del trattamento

I dati personali sono trattati con strumenti automatizzati e manuali per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Diritti degli interessati

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (articolo 7 del Codice in materia di protezione dei dati personali).

[36] Se si fa uso di cookie di profilazione, occorre rispettare quanto indicato dal Garante nel Provvedimento del 8 maggio 2014, GU n. 126 del 3 giugno 2014 - doc. web n. 3118884

Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Le richieste vanno rivolte:

- via e-mail, all'indirizzo: …….

- via fax: …….

- oppure via posta, a …….., Via …….

l'informativa e l'acquisizione del consenso all'atto della prenotazione o richiesta di disponibilità online

Il modello che segue, opportunamente verificato ed integrato, può essere inserito nella modulistica online di prenotazione o richiesta di disponibilità.

La informiamo che i dati da lei inseriti saranno trattati al solo fine di fornirle le informazioni richieste, ed eventualmente per definire/confermare la prenotazione di camere e altri servizi.

I suoi dati saranno trattati con mezzi informatici nel rispetto dei principi stabiliti dal Codice della Privacy (D. Legisl. 196/2003). Per ulteriori informazioni sulle modalità del trattamento, e per esercitare gli altri diritti a lei riconosciuti dall'articolo 7 del Codice della Privacy, potrà rivolgersi al Titolare …… o al Responsabile ……

Se è interessato a ricevere in futuro, all'indirizzo da lei indicato, la nostra newsletter / periodiche informative sulle nostre tariffe e offerte speciali, dovrà fornirci apposito consenso. Potrà comunque successivamente, in ogni momento, revocare tale consenso, rivolgendosi al Titolare o al Responsabile del trattamento.

- ☐ *prendo atto dell'informativa sopra riportata*
- ☐ *autorizzo l'invio di periodiche informative su tariffe e offerte speciali dell'albergo presso l'indirizzo da me indicato*

l'informativa ai lavoratori

Il modello di informativa che segue, da modificare o integrare a seconda delle specifiche esigenze, va consegnato ai lavoratori o reso loro disponibile.

Desideriamo informarla ai sensi dell'art. 13 del Codice sulla privacy (Decreto Legislativo 196/2003) che il trattamento dei suoi dati personali, da noi acquisiti, ha natura obbligatoria in quanto inerente, connesso e strumentale al suo rapporto di lavoro.

Tali dati vengono trattati, da noi e dai nostri incaricati, con sistemi informatici (e/o manuali) secondo i principi di correttezza, liceità e trasparenza previsti dal Codice sulla privacy, e tutelando la sua riservatezza ed i suoi diritti.

Il trattamento, nonché la comunicazione a soggetti diversi (enti previdenziali, enti bilaterali, fondi di previdenza e assistenza integrativa, pubbliche amministrazioni, eccetera) viene effettuato esclusivamente in adempimento alle normative vigenti ed alle disposizioni della contrattazione collettiva.

La informiamo inoltre che anche i suoi dati personali "sensibili", in quanto idonei a rivelare lo stato di salute o le convinzioni politiche, religiose o di altro genere, o l'adesione ad associazioni o sindacati, sono trattati al solo fine di adempiere agli obblighi derivanti dalle normative vigenti o dalle disposizioni della contrattazione collettiva, o in adempimento di sue specifiche richieste.

Per il trattamento di alcuni dati sensibili il Codice sulla privacy prevede il suo consenso scritto. Qualora ritenesse di non fornirlo, saremo costretti a sospendere l'effettuazione delle relative prestazioni.

In particolare, la informiamo che, ai fini di cui sopra, alcune operazioni di trattamento dei suoi dati sono effettuate da terzi, da noi incaricati, nel rispetto delle prescrizioni imposte dal Codice sulla privacy.

Per qualsiasi ulteriore informazione sulle modalità del trattamento potrà rivolgersi a ……, Titolare del trattamento (o eventualmente al Responsabile ……..).

l’acquisizione del consenso del lavoratore

Il modello che segue, opportunamente modificato e integrato a seconda delle specifiche esigenze, va sottoscritto dal lavoratore all’atto dell’assunzione.

Acquisite le informazioni relative al trattamento dei dati personali ai sensi dell'articolo 13 del Codice sulla privacy (Decreto Legislativo 196/2003), acconsento al trattamento dei miei dati sensibili per i soli fini previsti dalle normative vigenti e dalla contrattazione collettiva, o da me specificatamente richiesti.

Luogo e data .....……

Nome, cognome.....……

Firma .....

il conferimento delle credenziali di autenticazione agli addetti al ricevimento

Il modello che segue, opportunamente verificato ed integrato, può essere utilizzato per conferire l'incarico agli addetti al ricevimento di trattare i dati dei clienti, attribuendo loro le cosiddette "credenziali di autenticazione" (codice identificativo personale e password) previste dall'Allegato B del Codice.

Il sottoscritto ……Titolare / Responsabile dei trattamenti di dati personali, autorizza il Sig. …… ad effettuare le seguenti operazioni, connesse al normale svolgimento dell'attività aziendale:

- registrazione e notifica alla Questura delle generalità dei clienti alloggiati, rilevate dai documenti di riconoscimento da loro esibiti, in adempimento della normativa di polizia vigente (art. 109 Testo Unico delle leggi di polizia);
- registrazione dei dati dei clienti per espletare la funzione di ricevimento e per inoltrare messaggi e telefonate;
- registrazione dei dati necessari all'adempimento degli obblighi contabili e fiscali.

Per tali operazioni, da effettuare con correttezza e lecitamente, l'incaricato si avvarrà dell'ausilio di strumenti elettronici, e pertanto viene conferito il seguente CODICE IDENTIFICATIVO PERSONALE …….. e la seguente PASSWORD ……..

L'incaricato dovrà modificare la password al primo utilizzo e successivamente almeno ogni sei mesi.

La password, una volta modificata, dovrà essere comunicata al Sig. ……, incaricato della custodia delle copie delle credenziali di autenticazione.

Data e firma del sottoscritto ……..

Firma dell'incaricato per ricevuta……..

il conferimento dell'incarico di custode delle copie delle credenziali di autenticazione

Il modello che segue, opportunamente verificato ed integrato, può essere utilizzato per conferire ad un soggetto l'incarico di custodire copia delle "credenziali di autenticazione" (codice identificativo personale e password) assegnate ai lavoratori, ai sensi dell'Allegato B del Codice.

Il sottoscritto …… Titolare / Responsabile dei trattamenti di dati personali, conferisce al Sig. …… l'incarico di custodire le copie delle credenziali di autenticazione assegnate ai soggetti incaricati di trattamenti di dati personali effettuati con l'ausilio di strumenti elettronici.

Le credenziali di autenticazione appartenenti ad un incaricato potranno essere utilizzate solo in caso di sua assenza. L'incaricato dovrà comunque essere tempestivamente informato degli interventi effettuati.

Data e firma del sottoscritto

Firma dell'incaricato per ricevuta

l'attribuzione delle funzioni di amministratore di sistema

Riportiamo di seguito un modello per l'eventuale nomina dell'amministratore di sistema, da modificare ed integrare in relazione agli ambiti di operatività ed alle funzioni effettivamente svolte.

Il sottoscritto …… Titolare dei trattamenti di dati personali, considerando la sua esperienza, capacità e affidabilità, le conferisce la funzione di amministratore di sistema (AdS) nei seguenti ambiti di operatività:

- *gestione del sistema operativo*
- *gestione delle credenziali di autenticazione*
- *gestione del data base*
- *gestione delle reti*
- *gestione degli strumenti e apparati di sicurezza*
- *manutenzione hardware*

Nello svolgimento della funzione di AdS dovrà rispettare le vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza nonché le istruzioni impartite dal titolare o dal responsabile.

Le ricordiamo:

- *che il Suo operato sarà sottoposto a verifica da parte del Titolare o del Responsabile;*
- *che, a tal fine, saranno adottati sistemi per la registrazione degli accessi logici (autenticazioni informatiche);*
- *che i suoi estremi identificativi saranno riportati in un documento interno, disponibile in caso di accertamento da parte del Garante della protezione dei dati personali, e, nel caso in cui le sue mansioni riguardino anche indirettamente sistemi che permettano il trattamento di informazioni dei lavoratori, verranno resi conoscibili ai lavoratori medesimi;*
- *che l'attribuzione della funzione di AdS cessa in caso di attribuzione ad altro incarico che non preveda le attuali funzioni ovvero in caso di cessazione del suo rapporto di lavoro con l'azienda.*

Data e firma del Titolare ……

Firma dell'incaricato per ricevuta……

.

disciplinare aziendale in materia di utilizzo degli strumenti informatici

Il modello che segue, opportunamente modificato ed integrato, può essere utilizzato per informare i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica in azienda, e sulla possibilità che vengano effettuati controlli, come prescritto dal Garante[37].

Gentile Signora/Signor …….

la informiamo che gli strumenti che le vengono dati in uso per espletare la sua attività lavorativa (rete internet accessibile da postazione Client e servizio di posta elettronica) devono essere utilizzati con diligenza e correttezza, comportamenti che il lavoratore è sempre tenuto ad adottare nell'ambito del rapporto di lavoro.

Ogni utilizzo delle apparecchiature, degli elaboratori, delle reti e dei dati diverso rispetto alle finalità strettamente professionali deve essere limitato e occasionale. Poiché alcuni comportamenti possono mettere a rischio la sicurezza e l'immagine aziendale, anche nella normale attività lavorativa, di seguito vengono richiamate semplici regole procedurali finalizzate ad evitare condotte che inconsapevolmente possano causare rischi alla sicurezza del trattamento dei dati aziendali.

1. Posta Elettronica

Il servizio di posta elettronica aziendale è disponibile per ogni lavoratore in forma centralizzata e protetta.

Tale servizio è fruibile mediante specifico software client sia dall'Intranet che da Internet; è comunque possibile accedere via web alla casella personale.

Il servizio di posta elettronica aziendale non è un servizio in tempo reale, ovvero il tempo fra invio e ricezione di un messaggio non è istantaneo e dipende da molti fattori esterni.

L'invio di e-mail con allegati pesanti a mittenti multipli deve essere limitata onde evitare sovraccarico sul server centrale e sulle linee esterne.

In osservanza dei principi di pertinenza e non eccedenza, si adottano le seguenti misure di tipo organizzativo/tecnologico:

- *messa a disposizione di un indirizzo di posta elettronica condiviso per ufficio e/o servizio (ad esempio: segreteria@----------.it; helpdesk@----------it);*
- *attribuzione di un diverso indirizzo di posta elettronica destinato ad uso esclusivo del lavoratore;*
- *messa a disposizione di ciascun lavoratore di apposite funzionalità di sistema che consentono di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le coordinate di un altro soggetto o altre utili modalità di contatto presso l'azienda;*

[37] Provvedimento n. 13 del 1° marzo 2007, Gazzetta Ufficiale n. 58 del 10 marzo 2007 - doc. web n. 1387522

- *messa a disposizione di sistemi che consentono al lavoratore di delegare un collega a verificare il contenuto dei suoi messaggi e ad inoltrare quelli significativi per l'attività lavorativa, in caso di assenza improvvisa o prolungata del lavoratore;*
- *graduazione dei controlli che avverranno secondo le modalità di seguito indicate.*

L'utilizzo della posta elettronica interna contribuisce fortemente a rendere la comunicazione tempestiva, efficace ed economica. Il rispetto di alcune semplici regole può aiutare a migliorare ulteriormente l'utilizzo dello strumento. La casella di posta elettronica aziendale personale deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti.

E' possibile utilizzare la ricevuta di ritorno per avere la conferma della avvenuta lettura del messaggio da parte del destinatario.

L'utilizzo degli strumenti di comunicazione telematici deve necessariamente fare riferimento alle procedure in essere per quanto attiene alla verifica e circolazione delle comunicazioni prodotte o ricevute. In generale ogni comunicazione, inviata o ricevuta che abbia contenuti significativi o contenga impegni contrattuali o precontrattuali per l'azienda, deve essere visionata e autorizzata dal titolare dell'azienda o dal responsabile del servizio, o comunque deve essere rispettata la procedura in essere per la corrispondenza ordinaria.

E' fatto divieto di utilizzare la casella di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed espressa autorizzazione da parte del titolare dell'azienda o del responsabile del servizio.

E' in facoltà del lavoratore avere un proprio indirizzo elettronico presso sistemi esterni web; l'utilizzo di tale posta elettronica privata è consentito entro tollerabili limiti temporali.

E' da evitare la divulgazione degli indirizzi destinati alla ricezione di comunicazioni ufficiali. In caso di ricezione accidentale di messaggi di valenza ufficiale sulle caselle assegnate, gli assegnatari riceventi dovranno inoltrarli tempestivamente al titolare dell'azienda o al responsabile del servizio.

2. Antivirus

Tutti i computer aziendali (Client e P.C. portatili) sono dotati di apposito software che:

- *protegge in tempo reale il computer e i dati letti/scritti;*
- *può verificare che tutte le informazioni presenti nei dischi siano libere da virus;*
- *aggiorna automaticamente il dizionario dei virus; questa attività viene eseguita ad ogni collegamento alla Intranet aziendale;*
- *gestisce e rende visibile centralmente lo stato dei computer;*
- *distribuisce gli aggiornamenti mediante i server di sede.*

3. Utilizzo dell'elaboratore e della rete interna

L'accesso all'elaboratore, sia esso in rete o "stand alone", è sempre protetto da una o più password, così come previsto dalle misure minime di sicurezza disciplinate dal Codice della Privacy ed in particolare dall'Allegato B, denominato "Disciplinare tecnico in materia di misure minime di sicurezza".

La password deve essere composta da almeno n. 8 (otto) caratteri alfanumerici, oppure, nel caso in cui lo strumento elettronico non lo consenta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili all'incaricato (nome o data di nascita propri o dei propri familiari, nome del proprio cane o altri elementi simili) ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi (tre mesi in caso di trattamento di dati sensibili). Le password assegnate sono personali e non devono essere divulgate a terzi, fatta eccezione per il custode delle credenziali di autenticazione incaricato dall'azienda, e devono essere custodite dall'assegnatario con la massima diligenza.

Il lavoratore ha altresì l'obbligo di comunicare la password adottata ad ogni sua variazione, in busta chiusa firmata e datata di suo pugno, al custode delle credenziali di autenticazione incaricato dall'azienda. Il titolare dell'azienda o il responsabile del servizio, in caso di emergenza e/o di assenza del lavoratore, hanno il diritto di accedere al suo computer ed ai contenuti ivi custoditi per esigenze di carattere lavorativo, utilizzando la password comunicata al custode delle credenziali di autenticazione, e dando successiva comunicazione dell'avvenuto accesso al lavoratore.

Possono essere introdotte limitazioni all'accesso agli archivi aziendali, laddove il titolare dell'azienda o il responsabile del servizio lo ritengano opportuno.

E' tassativamente proibito installare programmi provenienti dall'esterno, in quanto l'utilizzo di software non regolarmente acquistato dall'azienda può configurare un reato, anche in considerazione del grave pericolo di contrarre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Le unità di rete sono aree di condivisione di informazioni strettamente aziendali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up da parte del titolare o persona da questi designata, che possono, in qualunque momento, procedere alla rimozione di ogni file o applicazione che riterranno pericolosi per la sicurezza o non inerenti all'attività lavorativa sia sui PC dei lavoratori sia sulle unità di rete.

Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante che non consenta in modo chiaro ed inequivocabile l'identificazione dello stato di revisione di un documento.

Il personal computer deve essere spento ogni sera prima di lasciare gli uffici e comunque protetto nelle pause durante l'orario di lavoro.

Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Tutti i supporti magnetici riutilizzabili (cd, dischetti, pendrive) contenenti dati personali devono essere trattati con particolare cautela. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione. Per questo motivo il supporto, al termine dell'utilizzo, deve essere formattato prima di essere riutilizzato oppure distrutto.

Il lavoratore avrà cura di effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla immediatamente dai vassoi delle stampanti comuni. Si eviterà in ogni modo e per quanto possibile, di dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (per esempio: corridoi, sale d'attesa, ecc.).

I fornitori esterni, addetti alla manutenzione di hardware, software e reti, operano in conformità alle presenti direttive, sotto la sorveglianza del titolare del trattamento dei dati personali o persona da questi designata.

4. Utilizzo della rete internet e dei relativi servizi

L'utilizzo imprudente di alcuni servizi della rete Internet, ancorché nell'ambito della normale attività aziendale, può essere fonte di particolari minacce alla sicurezza dei dati e all'immagine aziendale.

Seguono alcune semplici regole che devono essere osservate in tale circostanza.

Dall'interno della rete aziendale:

- *è da evitare l'upload e/o download di files e/o programmi software, anche gratuiti, se non per esigenze strettamente aziendali e fatti comunque salvi i casi di esplicita autorizzazione del titolare dell'azienda o del responsabile del servizio;*
- *è tassativamente proibita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal titolare dell'azienda o dal responsabile del servizio e con il rispetto delle normali procedure per gli acquisti;*
- *è vietata la partecipazione a forum non aziendali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività aziendale;*
- *è vietato l'uso della rete per accessi a servizi con finalità ludiche o estranei all'attività per tempi eccessivamente prolungati e comunque durante l'orario di servizio.*

5. Controlli e conservazione dei dati

Il titolare ha predisposto il proprio sistema informativo e la rete intranet ed internet al fine di utilizzare tali beni aziendali per esclusive esigenze organizzative e/o produttive.

A tal fine, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4 comma 2), di sistemi che consentono indirettamente un controllo a distanza (controlli preterintenzionali) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori; e ciò, anche in presenza di attività di controllo discontinue.

In particolare, tale attività di controllo potrà essere esercitata nel caso in cui si rivelino anomalie di funzionamento o si rendano necessarie attività di manutenzione o, comunque, in tutte le ipotesi in cui sia a rischio la sicurezza dei citati beni aziendali e/o la sicurezza sul lavoro in generale.

Questa attività di controllo a distanza sarà pertanto lecita e dettata dal principio di necessità. Il titolare dichiara di non utilizzare sistemi hardware e/o software idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:

- *la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;*
- *la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;*

- *la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo;*
- *l'analisi occulta dei computer portatili affidati in uso.*

Il titolare si riserva:

- *di effettuare controlli a campione, nel rispetto dei principi di pertinenza e non eccedenza, secondo le prescrizioni contenute nel presente disciplinare;*
- *di verificare comportamenti anomali, anche individuali, nel caso in cui un evento dannoso e/o una situazione di pericolo non siano stati impediti con i preventivi accorgimenti tecnici standard;*
- *di effettuare i controlli individuali su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree;*
- *di effettuare controlli anonimi causati da un rilevato utilizzo anomalo degli strumenti aziendali il cui esito deve essere comunicato tramite avviso generalizzato.*

Il titolare esclude la possibilità di effettuare controlli prolungati, costanti e/o indiscriminati.

In merito alla conservazione dei dati, il titolare adotta sistemi software programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata da una finalità specifica e comprovata e limitata nel tempo necessario a raggiungerla.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e avverrà solo in relazione:

- *ad esigenze tecniche o di sicurezza del tutto particolari;*
- *all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;*
- *all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria e della polizia giudiziaria. In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.*

6. PC Portatili

L'azienda consegna ad alcuni lavoratori i PC portatili, il cui utilizzo deve essere autorizzato dal titolare o dal responsabile del servizio. Le regole di utilizzo di queste apparecchiature sono le medesime indicate per i PC connessi alla rete.

I portatili che vengono sconnessi dalla rete aziendale e restano per lunghi periodi fuori dall'intranet, non ricevono gli aggiornamenti automatici e pertanto hanno un grado di protezione non allineato con gli standard aziendali.

7. Attività di formazione

L’azienda predispone regolari momenti formativi ed informativi per garantire a tutti i lavoratori incaricati il massimo aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.

Potrà comunque rivolgersi, per ogni chiarimento, al Titolare del trattamento …… o al Responsabile ……..

Firma per accettazione del lavoratore

Le guide degli alberghi

Ista, istituto di studi alberghieri intitolato a Giovanni Colombo, compianto presidente di Federalberghi, elabora analisi, indagini e ricerche sui temi di principale interesse per la categoria, autonomamente e in partnership con prestigiosi Istituti di ricerca.

L'antitrust sanziona Tripadvisor, 2015
Stop all'abusivismo, 2014 - 2015
Ospitare, servire, ristorare. Storia dei lavoratori di alberghi e ristoranti in Italia dalla fine dell'Ottocento alla metà del Novecento, 2014
Settimo rapporto sul sistema alberghiero italiano, 2014
L'appalto di servizi nelle aziende alberghiere, 2009 - 2014
@Hotel: digital marketing operations, 2014
L'alternanza scuola-lavoro nel settore turismo, 2014
I contratti a termine nel settore turismo dopo il jobs act, 2014
Il lavoro intermittente nel settore turismo, 2006 - 2014
Datatur, trend e statistiche sull'economia del turismo, 2011 - 2013 - 2014 - 2015
I tirocini formativi nel settore turismo, 2014
Agevolazioni fiscali sul gas naturale, 2014
Federalberghi ricorre all'Antitrust contro le on line travel agencies, 2014 - 2015
Guida al nuovo CCNL Turismo, 2014
L'imposta di soggiorno. Osservatorio sulla fiscalità locale, 2012 – 2014
Riflessioni e proposte per il rinnovo del CCNL Turismo, 2013
Osservatorio sul mercato del lavoro nel settore turismo, 2010 - 2012
Il lavoro delle donne nel settore turismo, 2012
Percorsi formativi in Italia per il settore turismo, 2012
La successione dei contratti a termine nel settore turismo, 2012
Il turismo lavora per l'Italia, 2012
Il lavoro accessorio nel Turismo, 2009 – 2011
La contrattazione di secondo livello nel settore turismo, 2011
Misure per l'incremento della produttività del lavoro, 2011
Gli stage nel settore turismo - ed. speciale progetto RE.LA.R., 2011
Gli stage nel settore turismo, 2004 - 2011
L'apprendistato stagionale dopo la riforma, 2011
La sicurezza antincendio negli alberghi italiani, 2011
Metodologia di sicurezza antincendio MBS, 2011
Imposta municipale unica, 2011
Guida al mercato russo, 2011
Il lavoro intermittente nel Turismo, 2009 – 2010
Guida al nuovo CCNL Turismo, 2010
L'apprendistato nel settore Turismo, 2010
Sesto rapporto sul sistema alberghiero, 2010
Indagine sui fabbisogni formativi nel settore Turismo, 2010
Agevolazioni fiscali sul gas naturale, 2010
La pulizia professionale delle camere albergo, 2009
L'appalto di servizi nelle aziende alberghiere, 2009
Gli ammortizzatori sociali nel settore Turismo, 2009

Il contratto di inserimento nel settore Turismo, 2009
Internet e Turismo, 2009
Guida al nuovo CCNL Turismo, 2007
Quinto rapporto sul sistema alberghiero, 2007
Mercato del lavoro e professioni nel settore Turismo, 2006
Come cambia il lavoro nel Turismo, 2006
Incentivi per le imprese nelle aree sottoutilizzate, 2006
Quarto rapporto sul sistema alberghiero, 2005
Il pronto soccorso nel settore Turismo, 2005
Dimensione dell'azienda turistica e agevolazioni pubbliche, 2005
La nuova disciplina del lavoro extra, 2004 – 2010
Dati essenziali sul movimento turistico, 2004
Dati essenziali sul movimento turistico nazionale ed internazionale, 2004
I contratti part time nel settore Turismo, 2004
I tirocini formativi nel settore Turismo, 2004
I condoni fiscali, 2003
Mercato del lavoro e professioni nel settore turismo, 2003
Repertorio dei percorsi formativi universitari per il settore turismo, 2003
Le attività di intrattenimento negli alberghi, 2003
La riforma dell'orario di lavoro, 2003
La riforma del part time, 2003
La privacy nell'ospitalità, 2002 – 2004
Terzo rapporto sul sistema alberghiero in Italia, 2002
I congedi parentali, 2002
Il turismo religioso in Italia, 2002
Il nuovo contratto di lavoro a termine, 2001 – 2002
Il nuovo collocamento dei disabili , 2001
Le stagioni dello sviluppo, 2001
Sistema ricettivo termale in Italia, 2001
Indagine sulla domanda turistica nei paesi esteri, 2001
Sistema ricettivo delle località termali in Italia, 2001
La flessibilità del mercato del lavoro, 2000
Osservatorio sulla fiscalità locale , 2000
Il Turismo lavora per l'Italia, 2000
Norme per il soggiorno degli stranieri, 2000
Indagine sulla domanda turistica nei paesi esteri, 2000
Secondo rapporto sul sistema alberghiero in Italia, 2000
Il codice del lavoro nel turismo, 1999 – 2003
Primo rapporto sul sistema alberghiero in Italia, 1999
Il collocamento obbligatorio, 1998
Manuale di corretta prassi igienica per la ristorazione, 1998
Diritti d'autore ed imposta spettacoli, 1997
La qualità e la certificazione ISO 9000 nell'azienda alberghiera, 1997
Il lavoro temporaneo, 1997
Analisi degli infortuni nel settore turismo, 1997
La prevenzione incendi negli alberghi: il registro dei controlli, 1996
La prevenzione incendi negli alberghi: come gestire la sicurezza, 1995
Il Turismo nelle politiche strutturali della UE, 1995
Il franchising nel settore alberghiero, 1995
Il finanziamento delle attività turistiche, 1994

Igiene e sanità negli alberghi, 1994
Linee guida per la costruzione di un modello di analisi del costo del lavoro, 1994
Costo e disciplina dei rapporti di lavoro negli alberghi dei Paesi CEE, 1993
Per una politica del turismo, 1993
Ecologia in albergo, 1993
Quale futuro per l'impresa alberghiera, 1993
La pulizia professionale delle camere d'albergo, 1993
Il turismo culturale in Italia, 1993
Il turismo marino in Italia, 1993
Serie storica dei minimi retributivi, 1993
Esame comparativo dei criteri di classificazione alberghiera, 1992
L'albergo impresa, 1990

Federalberghi da oltre cento anni è l'organizzazione nazionale maggiormente rappresentativa degli albergatori italiani.

La federazione rappresenta le esigenze e le proposte delle imprese alberghiere nei confronti delle istituzioni e delle organizzazioni politiche, economiche e sindacali.

Aderiscono a Federalberghi 131 Associazioni Territoriali, raggruppate in 19 Unioni Regionali, e 6 Sindacati Nazionali (Unione Nazionale Italiana Catene Alberghiere, Sindacato Grandi Alberghi, Sindacato Villaggi Turistici, Associazione Alberghi per la Gioventù, Federalberghi Isole Minori, Unihotel Franchising).

In seno a Federalberghi sono costituiti 5 Comitati Nazionali (Mezzogiorno, Attività stagionali, Attività termali, Consorzi alberghieri, Giovani albergatori)

FAIAT service srl è il braccio operativo di Federalberghi.

Presidente di Federalberghi è Bernabò Bocca.
Il Direttore Generale è Alessandro Massimo Nucara.

Federalberghi aderisce dal 1950 a Confcommercio ove, insieme alle principali federazioni di categoria che operano nel Turismo, ha dato vita a Confturismo, l'organizzazione di rappresentanza imprenditoriale di settore.

Federalberghi è socio fondatore di Hotrec, la Confederazione Europea degli imprenditori del settore alberghiero e della ristorazione.