

**LA PROTEZIONE DEI DATI PERSONALI  
NELLA GESTIONE DELLE IMPRESE  
RICETTIVE**

la privacy nell'ospitalità

seconda edizione

Federica Bonafaccia

EDIZIONI ISTA  
Istituto Internazionale di Studi  
e Documentazione Turistico Alberghiera  
00187 Roma – Via Toscana 1

Progetto grafico di Noemi Moauro.

Tipografia Copygraphic, Roma.  
Finito di stampare nel mese di settembre 2004.

## **Premessa**

La normativa sulla “Protezione dei dati personali”, comunemente chiamata normativa sulla privacy, emanata al fine di garantire il rispetto dei diritti di riservatezza delle persone, ha creato nel mondo dell’ospitalità moltissimi problemi.

All’esito della sua emanazione, infatti, la sua complessità e contraddittorietà ha rischiato di paralizzare ogni attività economica. La mancanza di chiarimenti da parte del neonato Ufficio del Garante e la necessità di assicurare comunque la sua applicazione, data la rilevanza delle sanzioni previste, ha portato inizialmente a conseguenze paradossali.

Nonostante le molte modifiche e semplificazioni, e nonostante il recente accorpamento dell’intera materia in un Codice, l’argomento è ancora fortemente temuto dai nostri imprenditori, data la onerosità delle sanzioni previste.

Grazie alla particolare esperienza maturata su tali problematiche, abbiamo realizzato questa guida, specifica per le aziende ricettive, con l’auspicio di dare un contributo fattivo per una applicazione logica e razionale della normativa.

IL PRESIDENTE

Bernabò Bocca





## INDICE

Premessa .....	3
<b>INTRODUZIONE .....</b>	<b>7</b>
il diritto alla “privacy” .....	9
il diritto alla “privacy” nel campo dell’ospitalità .....	12
<b>IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (Decreto Legislativo 196/2003).....</b>	<b>15</b>
la struttura del Codice .....	17
la finalità della normativa .....	18
le definizioni .....	20
il campo di applicazione .....	23
il Garante .....	24
le forme di tutela .....	25
i diritti dell’interessato .....	28
l’informativa .....	30
il consenso .....	33
la notificazione al Garante .....	37
il trasferimento di dati personali all’estero .....	40
le garanzie per i dati sensibili .....	41
le deleghe di responsabilità ed il conferimento di incarichi.....	48
le modalità di raccolta e requisiti dei dati .....	50
le misure di sicurezza.....	51
il trattamento non automatizzato di dati personali non sensibili....	53
trattamento non automatizzato di dati personali sensibili .....	54
il trattamento automatizzato di dati personali non sensibili.....	55
trattamento automatizzato di dati personali sensibili .....	57
il documento programmatico sulla sicurezza .....	58
la disciplina transitoria.....	60
la privacy nella comunicazione elettronica.....	61
la videosorveglianza .....	65
<b>ANALISI DEI TRATTAMENTI TIPICI DELLE AZIENDE RICETTIVE .....</b>	<b>69</b>
la prenotazione.....	71
la registrazione a fini di polizia.....	73
iniziative promozionali e pubblicitarie .....	75
servizio di ricevimento e portineria .....	76
trattamento dei dati relativi ai lavoratori.....	78
trattamento dei dati relativi ai fornitori.....	79
trattamento dei dati relativi ad agenzie di viaggi o tour operator ..	80

<b>I FACSIMILI.....</b>	<b>81</b>
l'articolo 7 .....	83
il trattamento dei dati dei clienti .....	84
l'informativa e l'acquisizione del consenso per il trattamento dei dati dei lavoratori.....	87
il conferimento del codice identificativo personale e della chiave di accesso.....	89
il conferimento dell'incarico di custode delle copie delle credenziali di autenticazione.....	91
il documento programmatico sulla sicurezza.....	92
<b>GLI ALLEGATI.....</b>	<b>101</b>
il decreto legislativo 30 giugno 2003 n. 196 (stralcio).....	103
la deliberazione 31 marzo 2004, n. 1 - "Casi da sottrarre all'obbligo di notificazione al Garante".....	153
autorizzazione n. 1/2004 al trattamento dei dati sensibili nei rapporti di lavoro .....	156
autorizzazione n. 5/2004 al trattamento dei dati sensibili da parte di diverse categorie di titolari .....	162
le guide degli alberghi .....	171

## **INTRODUZIONE**



## **il diritto alla “privacy”**

L'8 maggio del 1997 è entrata in vigore la legge n.675 del 31 dicembre 1996 sulla protezione dei dati personali, comunemente detta legge sulla “privacy”. Si è trattato di un avvenimento molto importante per il nostro ordinamento giuridico, ma anche per tutti noi cittadini, per le imprese, per gli enti e le associazioni. Una piccola rivoluzione destinata a scardinare la comune percezione del concetto di riservatezza.

Il diritto alla riservatezza, anche a causa dell'impetuoso sviluppo tecnologico, è diventato in questi ultimi anni un baluardo di civiltà, ed i cittadini mostrano assai più di prima di preoccuparsi del trattamento elettronico delle loro informazioni. Le persone sono ormai conosciute quasi esclusivamente attraverso i dati che le riguardano e che fanno di esse una entità astratta. Da qui l'esigenza di controllare le modalità attraverso le quali queste informazioni vengono trattate, collegate, fatte circolare, e da qui l'esigenza di disporre di una legge sulla “privacy”.

Una legge sulla “privacy” era quindi necessaria per garantire ai cittadini italiani il pieno rispetto del diritto alla riservatezza attribuito loro dalla Costituzione, ed annoverato tra i diritti inviolabili dell'uomo.

Una legge sulla “privacy” era anche necessaria per recepire una direttiva europea. Per l'ordinamento italiano il recepimento della direttiva ha costituito un adempimento di grande rilievo, consentendo di colmare le differenze con gli altri ordinamenti della Comunità. Il ritardo italiano ha infatti penalizzato non solo i singoli individui, che non potevano contare sulla protezione delle loro libertà individuali e sulle stesse garanzie assicurate ai cittadini degli Stati membri, ma anche gli stessi operatori economici, i quali non potevano avvalersi di dati provenienti dagli altri Paesi europei perché non erano in grado di garantire la stessa protezione.

Una legge sulla “privacy” era quindi necessaria per ragioni di civiltà giuridica, per tutelare i diritti inviolabili degli individui e per tutelare gli interessi economici raccolti intorno alle banche dati.

Una legge sulla “privacy” era infine necessaria per consentire all’Italia di entrare pienamente nell’area Schengen. L’approvazione di una legge di protezione dei dati personali era infatti condizione necessaria ed indispensabile per consentire all’Italia la piena attuazione dell’Accordo di Schengen sull’eliminazione graduale dei controlli alle frontiere comuni.

La legge sulla “privacy”, comunque, avrebbe potuto limitarsi a stabilire solo alcune norme di sicurezza nel trattamento di dati personali, ma il Legislatore ha invece optato per una legge ambiziosa negli obiettivi e complessa nella struttura, che ha sicuramente portato un aggravio burocratico non indifferente per le imprese, contrariamente alle scelte operate in altri Paesi europei ed in stridente contrasto con il processo di semplificazione in corso.

La legge sulla privacy ha avuto bisogno di più di una revisione e limatura, indispensabili per consentirne il concreto rispetto da parte di tutti.

Da una privacy un po’ “utopistica”, quale quella che si intendeva raggiungere con il testo iniziale della legge, siamo gradatamente passati ad una privacy “possibile”, quale quella ora sicuramente realizzabile grazie alle ultime modifiche apportate dal Decreto legislativo 196/2003, con cui l’intera materia è stata razionalizzata e semplificata all’interno del “Codice in materia di protezione di dati personali”.

Le nuove norme si ispirano ad un modello che tiene maggiormente conto della realtà e che cerca di risolvere il problema centrale della reale efficacia delle regole. Ma nessuno sconto è stato fatto rispetto all’impostazione iniziale.

La privacy resta un argomento delicatissimo e trattato con estremo rigore dalle nostre Istituzioni. Il nuovo Codice continua comunque a

richiedere numerosi adempimenti alle imprese finalizzati a tutelare il diritto alla riservatezza delle persone fisiche e giuridiche.

Ma è cambiato l'approccio, basato meno sulla forma e più sulla sostanza. Migliore bilanciamento tra i diversi valori, previsioni di buon senso più facilmente applicabili che in passato, maggiore riconoscimento al ruolo dell'autoregolamentazione, sanzioni meno penalizzanti.

L'articolo 1 del nuovo Codice contiene una importante dichiarazione di principio secondo cui "Chiunque ha diritto alla protezione dei dati personali che lo riguardano". Viene quindi espressamente codificato un importante diritto soggettivo, che nella legge 675/1996 era riconosciuto solo implicitamente.

Il diritto alla protezione dei dati personali viene temperato dai successivi articoli 2 e 3 del Codice, nei quali da una parte si riconosce la necessità di effettuare trattamenti di dati personali, dall'altra si tende a garantire che gli stessi avvengano "nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato".

Il nuovo Codice vuole inoltre garantire un elevato livello di tutela dei diritti e delle libertà dell'interessato, secondo modalità che devono essere esercitabili in modo semplice ed efficace dall'interessato, riconoscendo nel contempo la necessità di semplificare anche gli obblighi di coloro che effettuano il trattamento.

Per quanto riguarda le modalità di esercizio della tutela e gli adempimenti per coloro che effettuano i trattamenti, il nuovo Codice ha essenzialmente riscritto la precedente normativa che ora risulta di più agevole lettura e non lascia spazio, o almeno ne lascia poco, ad interpretazioni penalizzanti.

Tutto ciò, ci auguriamo, permetterà di evitare le applicazioni troppo rigide delle norme che hanno spesso reso la legge impervia e ricca di paradossi.

## **il diritto alla “privacy” nel campo dell’ospitalità**

Non è facile spiegare al gestore di una struttura ricettiva a cosa serve una legge sulla “privacy” ed a cosa servono gli obblighi connessi con la sua entrata in vigore.

Non è facile spiegare ad un albergatore, così come ad un campeggiatore o ad un affittacamere, perché una legge così complicata, ricca di contraddizioni, abbia burocratizzato in complesse ed inutili registrazioni uno dei suoi fondamentali doveri: garantire al cliente la più ampia riservatezza durante tutto il suo soggiorno.

Anche senza una legge sulla “privacy” il cliente ha sempre goduto di un sufficiente ed adeguato grado di riservatezza durante il suo soggiorno in una struttura ricettiva, sia essa albergo o residence, campeggio o villaggio turistico, affittacamere o bed & breakfast.

Tale grado di riservatezza, ritenuto sufficiente ed adeguato, si basa da sempre sull’esperienza e la conoscenza che gli imprenditori del settore hanno delle esigenze della propria clientela.

All’interno di una struttura ricettiva, infatti, la tutela della riservatezza deve fare i conti con la prestazione del servizio di alloggio, che impone alcune intromissioni nella sfera privata del clienti, ben conosciute ed implicitamente accettate. Tali intromissioni sono alcune volte imposte dalla legge, altre imposte dalla natura stessa della prestazione, altre sono invece richieste dal cliente stesso.

Il grado di riservatezza da sempre assicurato al cliente è quindi “standardizzato” sulla base dell’esperienza delle comuni esigenze della clientela ed è variabile a seconda della tipologia di struttura ricettiva e della sua categoria. Può ovviamente aumentare o diminuire a seconda di particolari necessità dei clienti, e delle eventuali richieste di maggiore o minore protezione della propria sfera privata.

A seguito dell’entrata in vigore della legge sulla “privacy” gli

imprenditori del settore sono stati costretti a ripensare il loro servizio, trovando un nuovo difficile equilibrio tra il rispetto delle prescrizioni di legge e la soddisfazione delle esigenze dei clienti.

La tutela “standardizzata” della riservatezza, così come il consenso implicito dei clienti alle intromissioni nella loro sfera privata sono infatti concetti inconciliabili con lo spirito della legge. E per rispettare la legge, l'imprenditore è spesso costretto a non fornire servizi graditi ai clienti, quando non ha modo di acquisire il loro consenso e di documentarlo per iscritto così come richiesto dalla normativa.

La normativa sulla “privacy”, quindi, non può certo garantire al cliente una maggiore riservatezza rispetto a quanto avveniva prima della sua entrata in vigore. Ma garantisce sicuramente al cliente un supplemento di fastidio in più al suo arrivo in una struttura ricettiva.

Oltre alla seccatura di esibire il proprio documento, compilare e firmare la scheda di polizia, la legge ritiene infatti che sia un comportamento civile, oltre che un obbligo di legge, costringere i clienti ad ascoltare con pazienza, anche se non ne hanno alcuna voglia, le informazioni sulle modalità del trattamento dei loro dati personali; costringerli a documentare per iscritto che non hanno nulla da nascondere, e che quindi acconsentono a ricevere telefonate e messaggi durante il loro soggiorno; costringerli a firmare un apposito modulo se vogliono ricevere gli auguri di Natale con l'aggiornamento delle tariffe.

Ma vediamo più nel concreto come è articolata la normativa e quali sono i principali adempimenti a cui gli imprenditori del settore ricettivo sono tenuti in seguito della sua entrata in vigore.



**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 nuovo “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.

L’emanazione di un Codice unitario ed organico si è resa necessaria per coordinare le varie disposizioni legislative e regolamentari emanate in materia di privacy nel corso di questi ultimi anni e per apportare alle stesse le integrazioni e modificazioni indispensabili per assicurare alla normativa la migliore attuazione, anche alla luce dell’opera interpretativa svolta dal 1996 ad oggi dall’Autorità Garante.

Il Codice presenta una più razionale articolazione, ed 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, 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 abrogative, transitorie e finali.

Seguono una serie di allegati (codici di deontologia e buona condotta, 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<sup>1</sup>, 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 fisiche e giuridiche (comprese quindi le società di capitali, le associazioni riconosciute e gli enti dotati di personalità giuridica) costituisce un diritto assoluto ed inviolabile, meritevole di tutela attraverso la comminazione di sanzioni civili, penali ed amministrative.

Rispetto alla direttiva comunitaria, la normativa italiana ha voluto estendere la tutela anche ai dati personali delle persone giuridiche, oltre che delle persone fisiche, suscitando perplessità e dubbi tra gli stessi parlamentari.

Ai dati delle persone giuridiche è comunque attribuita nel concreto una tutela affievolita, sicuramente non paragonabile a quella che la normativa intende assicurare ai dati delle persone fisiche.

Ci si è ispirati quindi, in più punti, a criteri più rigorosi rispetto a quelli dettati in sede comunitaria e già presenti nelle legislazioni di taluni Stati membri.

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;

---

<sup>1</sup> 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.

- 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.

E se la tutela della riservatezza è concepibile solo per le persone fisiche, il diritto all'identità personale può sicuramente riguardare anche le persone giuridiche.

## le definizioni

Per comprendere la reale portata della normativa, è indispensabile analizzare alcune definizioni 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, persona giuridica, ente od associazione, identificati o identificabili, 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.

*“Dato anonimo”*: il dato che in origine o a seguito di trattamento non può essere associato ad un interessato identificato o identificabile.

*“Titolare”*: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente 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 a compiere operazioni di trattamento dal titolare o dal responsabile;

*"Interessato"*: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

*"Comunicazione"*: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, 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.

*"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 per la tutela delle persone e di altri soggetti rispetto al trattamento di dati personali, che opera in piena autonomia e indipendenza.

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 elaborazione 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) 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: Prof. Stefano Rodotà (*Presidente*), Prof. Giuseppe Santaniello (*vice Presidente*), Dott. Mauro Paissan, Prof. Gaetano Rasi. Il Segretario Generale è il Dott. Giovanni Buttarelli.

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 regola 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 regola 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 e' 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 responsabile del trattamento di dar luogo all'adesione spontanea 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**

Secondo l'articolo 7 del Codice, l'interessato ha il diritto:

- di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano;
- 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;
- 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 agli altrui possibili abusi conseguenti ad un illecito trattamento del dato.

La possibilità di verifica dell'esistenza dei dati avviene attraverso l'accesso al registro presso il Garante. Tale accesso, che è gratuito,

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: 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.

Tuttavia, questi strumenti attivi di tutela dei diritti dell'interessato necessitano di essere calibrati perché vi sia un'equa corrispondenza tra il loro costo (incluse le perdite connesse con il mancato utilizzo dei dati da parte del titolare del trattamento) e la tutela reale che offrono.

Ancora una volta, la possibilità di raggiungere un buon risultato è connessa con un uso equilibrato di tali strumenti, non eccessivo ma neanche scarso.

## **P'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 essere previamente informato, oralmente o per iscritto:

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

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;
- il trattamento è connesso allo svolgimento delle "investigazioni difensive" in materia penale (art. 38 norme di attuazione del c.p.p.) o alla difesa di un diritto in sede giudiziaria (a meno che il trattamento si protragga per un periodo superiore a quello strettamente necessario al perseguimento di tali finalità o sia svolto per ulteriori scopi);
- l'informativa all'interessato comporti un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto

tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

Tali circostanze, previste nell'ultimo punto, saranno 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 giudiziarie.

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 la mancata osservanza delle disposizioni relative alla corretta informativa con la sanzione amministrativa da 3.000 a 18.000 Euro, quasi il doppio della sanzione prevista nella precedente Legge 675/1996.

Nel caso di non corretta informativa relativa al trattamento di dati cosiddetti "sensibili", di cui parleremo in seguito, o di trattamenti che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, o comunque nei casi di maggiore rilevanza del pregiudizio per uno o più interessati, la somma applicabile come sanzione varia da 5.000 a 30.000 Euro.

Tali sanzioni possono essere aumentate fino al triplo quando esse risultino inefficaci in ragione delle condizioni economiche del contravventore.

## **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 riguardi dati sensibili.

L'articolo 24 del Codice consente il trattamento anche senza il 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.

L'articolo 25 del Codice stabilisce infine che i dati personali non possano 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<sup>2</sup>, 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

---

<sup>2</sup> Decisione del Garante per la protezione dei dati personali del 28.5.1997, relativa ai moduli di informativa adottati dalla Banca Nazionale del Lavoro.

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.

## 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 casi di trattamenti sottoposti all'obbligo di notificazione. Il Garante ha inoltre provveduto con apposita Deliberazione<sup>3</sup> 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 alberghiere, 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;
- trattamento dei dati dei clienti effettuato per l'invio di materiale pubblicitario o per iniziative promozionali;

---

<sup>3</sup> 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 lavoratori;
- trattamento dei dati dei fornitori;
- trattamento dei dati delle agenzie di viaggi o tour operator.

Con una ulteriore nota sull'argomento, il Garante ha provveduto inoltre a chiarire:

- per quanto riguarda la localizzazione di persone o oggetti 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 ora possibile solo per via telematica e con sottoscrizione con firma digitale ([www.garanteprivacy.it](http://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 10.000 euro a 60.000 euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

L'articolo 168 del Codice, inoltre, 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 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;
- concerne dati riguardanti persone giuridiche, enti o associazioni.

## 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 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.

L’articolo 26 prevede in alcuni casi la possibilità di trattare i dati sensibili anche senza consenso dell’interessato, 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 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 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 del 30.6.2004<sup>4</sup> 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,

---

<sup>4</sup> Pubblicata nella G.U. n. 190 del 14 agosto 2004

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. 5/2004 ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005. Il Garante ha comunque previsto la possibilità per i titolari di adeguarsi alle prescrizioni ivi contenute entro il 30 settembre 2004.

Con l'autorizzazione n. 1 del 30.6.2004<sup>5</sup> il Garante ha invece legittimato il trattamento di dati sensibili finalizzato alla gestione dei rapporti di lavoro.

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;

---

<sup>5</sup> Pubblicata nella G.U. n. 190 del 14 agosto 2004

- 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, semprechè 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. 5/2004

L'autorizzazione n. 1/2004 ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005. Il Garante ha comunque previsto la possibilità per i datori di lavoro di adeguarsi alle prescrizioni ivi contenute entro il 30 settembre 2004.

**Le sanzioni** – Nel caso di non corretta informativa relativa al trattamento di dati sensibili, l'articolo 161 del Codice prevede che il titolare del trattamento sia punito con la sanzione amministrativa variabile da 5.000 a 30.000 Euro. La sanzione può essere aumentata fino al triplo quando essa risulti inefficace in ragione delle condizioni economiche del contravventore.

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 violazione 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 intendesse 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 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 del 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 della 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<sup>6</sup> 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

---

<sup>6</sup> 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.

- 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 alle modalità con cui viene effettuato il trattamento ed al 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 un iter procedimentale la cui osservanza viene rafforzata mediante appunto la previsione di idonee misure di sicurezza.

**Le sanzioni** - La mancata adozione delle misure minime di sicurezza costituisce illecito penale punibile con l'arresto sino a due anni o con l'ammenda da diecimila a cinquantamila euro. 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.

## **il trattamento non automatizzato di dati personali non sensibili**

- Ad esempio: dati dei clienti ai fini della notifica alla polizia (schede di 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.

## **trattamento non automatizzato di dati personali sensibili**

- Ad esempio: dati sull'adesione a sindacati da parte dei lavoratori 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 automatizzato di dati personali non sensibili**

- Ad esempio: dati dei clienti ai fini della notifica alla polizia (schede di 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 soggetto che ha l'accesso al trattamento di determinate informazioni deve averne assoluta necessità in ragione della sua attività e deve superare un duplice controllo che consiste in una **verifica di autenticazione**, 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.
- *Autenticazione* - Rappresenta un primo livello di controllo. Il Disciplinare Tecnico (Allegato B) prevede infatti che un soggetto, per poter accedere ad uno strumento informatico per trattare dati personali, deve essere in possesso delle c.d. **credenziali di autenticazione**. Le credenziali di autenticazione possono essere costituite dalla combinazione di un'utenza individuale (user-id), associata ad una parola chiave (password). La parola chiave deve essere mantenuta segreta e deve essere di almeno 8 caratteri (o pari al numero massimo di caratteri consentito dal sistema), non deve contenere riferimenti agevolmente riconducibili al soggetto, deve essere modificata dallo stesso al primo utilizzo e successivamente almeno ogni 6 mesi. Devono essere impartite ai soggetti incaricati del trattamento opportune istruzioni affinché non venga lasciato incustodito e accessibile a terzi lo strumento elettronico durante una sessione del trattamento. Quando l'accesso ai dati o allo strumento elettronico è consentito solo utilizzando la parola chiave dell'incaricato, il titolare del trattamento deve

individuare per iscritto i soggetti incaricati della custodia delle copie delle credenziali, da utilizzare solo in caso di assenza dell'incaricato, che deve comunque essere tempestivamente informato degli interventi effettuati. Le credenziali di autenticazione non utilizzate da almeno sei mesi debbono essere disattivate, salvo in caso di un utilizzo occasionale meramente finalizzato alla gestione tecnica. Le credenziali possono essere costituite anche da un dispositivo di autenticazione o da una caratteristica biometrica (impronta digitale).

- *Autorizzazione* – Occorre ricorrere ad un sistema di autorizzazione nel caso in cui vi siano diversi incaricati per diversi ambiti del trattamento. In tal caso, oltre all'autenticazione per consentire l'accesso allo strumento elettronico, è necessario attribuire l'autorizzazione allo specifico ambito del trattamento, in modo da consentire l'accesso ai soli dati necessari per effettuare le operazioni di trattamento assegnate. Periodicamente, e comunque almeno annualmente, va verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
- *Protezione dei dati* - 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.
- *Attestato di conformità* - 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 attestino la conformità al disciplinare tecnico del Codice.

## **trattamento automatizzato 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.
- il titolare del trattamento è tenuto a redigere annualmente, entro il 31 marzo, un **documento programmatico sulla sicurezza**, di cui dovrà fare menzione nella relazione accompagnatoria del bilancio d'esercizio.

## il documento programmatico sulla sicurezza

Nel caso di trattamenti di dati sensibili (o di dati giudiziari, che le aziende ricettive però non trattano) con l'ausilio di strumenti elettronici, il titolare è tenuto a redigere annualmente (entro il 31 marzo) un **documento programmatico sulla sicurezza**, di cui dovrà fare menzione nella relazione accompagnatoria del bilancio d'esercizio.

In via transitoria, il DPS dovrà essere realizzato per la prima volta entro il 31 dicembre 2004.

Ricordiamo che il cosiddetto **DPS** va obbligatoriamente redatto solo nel caso di trattamenti di dati sensibili o di dati giudiziari con l'ausilio di strumenti elettronici. La redazione del documento programmatico sulla sicurezza non è invece necessaria in caso di trattamenti di dati sensibili o giudiziari effettuato in forma cartacea.

Ricordiamo anche che sono considerati "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.

Il DPS deve contenere:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;

- la previsione di interventi formativi degli incaricati del trattamento. La formazione deve essere programmata già al momento dell'ingresso in servizio o in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno della struttura del titolare.

Al fine di fornire un contributo utile alla redazione ed all'aggiornamento del Documento programmatico sulla sicurezza, soprattutto nelle realtà di piccola e media dimensione, il Garante ha emanato una apposita **Guida operativa**<sup>7</sup>, utilizzabile facoltativamente.

Sulla base delle indicazioni riportate nella Guida del Garante, abbiamo elaborato un modello di DPS che troverete nel capitolo dedicato ai facsimili. Il modello, opportunamente modificato ed integrato secondo le peculiarità dell'organizzazione del lavoro e tecnica della azienda, può essere utilizzato per la redazione del DPS.

---

<sup>7</sup> La guida alla redazione del DPS è stata emanata con provvedimento del garante lo scorso 11 giugno 2004, dopo una consultazione pubblica, ed è scaricabile dal sito [www.garanteprivacy.it](http://www.garanteprivacy.it).

## la disciplina transitoria

L'articolo 180 del Codice ha inizialmente previsto, in via transitoria, che **le nuove misure di sicurezza**, non previste dalla previgente disciplina, andassero adottate entro il 30 giugno 2004. Con il decreto legge 24 giugno 2004 n. 158<sup>8</sup> il Consiglio dei Ministri ha però prorogato tale termine.

Sono slittati infatti dal 30 giugno al 31 dicembre 2004 i termini per applicare le misure di sicurezza da parte di tutti coloro che trattano dati personali. Come riportato nei precedenti capitoli, le misure di sicurezza sono previste dagli articoli da 33 a 36 del Codice e dal Disciplinare Tecnico contenuto nell'Allegato B.

Il decreto legge 158/2004 ha previsto inoltre che il titolare dei trattamenti di dati personali, i cui strumenti elettronici non consentano tecnicamente in tutto in parte l'immediata applicazione delle misure di sicurezza previste dal Codice, avrà tempo fino al 31 marzo 2005 per adeguare i propri strumenti ed applicare le misure di sicurezza. In tal caso dovrà però descrivere tali obiettive ragioni tecniche in un documento di data certa (ad esempio la raccomandata a sé stesso) da redigere entro il 31 dicembre 2004 e da conservare presso la propria struttura. Nel frattempo, dovrà adottare ogni possibile misura di sicurezza per evitare un incremento dei rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'articolo 181, comma 1, lett. c), del Codice ha invece fissato la data del 30 aprile 2004 per effettuare o rinnovare **la notificazione al Garante**, da effettuare nei soli casi previsti dall'articolo 37. La notificazione è ora possibile solo per via telematica e con sottoscrizione con firma digitale.

---

<sup>8</sup> Convertito dal Parlamento nella Legge 27 luglio 2004 n. 188, pubblicata nella G.U. n. 177 del 30 luglio 2004.

## **la privacy nella comunicazione elettronica**

Il titolo X del Codice, articoli da 121 a 134, regola 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 telefoniche riservate e sicure, impedendo inoltre le chiamate telefoniche ed i fax pubblicitari indesiderati ed i trasferimenti di chiamata inopportuni, e riconosce anche il diritto degli abbonati 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 attendendosi a particolari cautele.

Sintetizziamo di seguito alcune delle più rilevanti disposizioni:

**Dati sul traffico e fatturazione** - I dati sul traffico relativo agli abbonati e 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'abbonato 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 trenta mesi, per finalità di accertamento e repressione di reati, secondo le modalità individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante.

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

**Chiamate di disturbo** - L'abbonato 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 abbonato, 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 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 abbonati, e se possibile gli utenti, qualora ci sia la possibilità che soggetti ad esso estranei ascoltino non intenzionalmente il contenuto di comunicazioni o conversazioni.

L'abbonato deve informare l'utente quando lo stesso rischio ricorra per le comunicazioni effettuate dall'utente presso la sede dell'abbonato.

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

**Sanzioni** - Se dal fatto deriva documento, colui che, al fine di trarne profitto per sé o per altri o di recare ad altri un danno, procede al trattamento illecito di dati è punito con la reclusione da 6 a 18 mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da 6 a 24 mesi.

## la videosorveglianza

Con un provvedimento del 29 aprile 2004, il Garante per la privacy ha emanato alcune disposizioni in materia di videosorveglianza, ispirandosi alle indicazioni espresse sulla materia in varie sedi internazionali e comunitarie.

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.

**Principi di liceità e proporzionalità** - In linea generale il Garante, nel dettare la disciplina della videosorveglianza, ha tenuto in considerazione il fine cui essa è diretta, mostrando di comprendere la necessità del suo utilizzo quando si devono difendere legittimi interessi, quali la sicurezza all'interno e all'esterno di edifici dove si svolgono per esempio attività commerciali, e di conseguenza anche attività ricettive.

A tal fine ha individuato due principi che devono essere osservati affinché la videosorveglianza sia legittima: la liceità e la proporzionalità.

Il principio di liceità consente la raccolta e l'uso delle immagini qualora essi siano necessari per adempiere ad obblighi di legge o siano effettuati per tutelare un legittimo interesse. Di conseguenza è consentita la videosorveglianza, senza necessità di alcun consenso, qualora essa sia effettuata nell'intento di perseguire fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione di incendi, sicurezza del lavoro, etc.

La raccolta e l'uso delle immagini, tuttavia, deve essere proporzionale agli scopi perseguiti. Il principio di proporzionalità, pur consentendo

marginari di libertà nella valutazione da parte del titolare del trattamento, non comporta però scelte del tutto discrezionali ed insindacabili.

Gli impianti di videosorveglianza possono essere infatti attivati solo quando altre misure siano state ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione dei beni, anche in relazione agli interessi sopra indicati (per esempio, la sicurezza), devono risultare comunque inefficaci altri idonei accorgimenti (per esempio, controlli da parte di addetti e sistemi di allarme). Ma la presenza di un addetto alla sicurezza all'ingresso di un albergo non rende illegittima la installazione di impianti di videosorveglianza, ben essendo possibile che il furto sia consumato all'interno della stessa struttura, prima dell'uscita dalla stessa.

Alla luce di tali principi, il fine di garantire una adeguata tutela dell'interesse alla sicurezza delle strutture ricettive, esposte a rischio di attività criminali in ragione della detenzione di denaro, valori o altri beni, andrà bilanciato con l'interesse dei soggetti che vi accedono. Il provvedimento, pertanto, si preoccupa di disciplinare anche l'utilizzo dei dati raccolti.

**Oggetto delle riprese** - Nell'uso delle apparecchiature volte a riprendere 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 di visuale all'area effettivamente da proteggere, evitando la ripresa di luoghi circostanti e di particolari non rilevanti (per esempio, vie, esercizi commerciali, edifici, etc).

Per quanto attiene ai rapporti di lavoro, nell'attività di videosorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa. Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro.

E' inammissibile la installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività

lavorativa.

**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.

Un eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia delle registrazioni su specifica richiesta dall'autorità giudiziaria in relazione ad un'attività investigativa in corso.

Le ragioni delle scelte in ordine al se ed ai tempi di conservazione dei dati devono essere adeguatamente documentate in un atto autonomo conservato presso il titolare ed il responsabile del trattamento e ciò anche ai fini della eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso.

Il sistema impiegato deve essere programmato in modo da consentire la cancellazione automatica da ogni supporto.

**Adempimenti** - Il soggetto che intende installare un sistema di videosorveglianza deve eseguire i seguenti adempimenti:

Informativa – Occorre informare gli interessati che stanno per accedere o che si trovano in una zona videosorvegliata della presenza del sistema e della eventuale registrazione delle immagini che li riguardano.

Il supporto con l'informativa:

- deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile.

A tal fine il Garante ha inserito nel provvedimento un modello semplificato di informativa, utilizzabile a discrezione del titolare del trattamento. Gli eventuali altri modelli già in uso o che si volessero utilizzare in futuro, pertanto, sono consentiti.

Prescrizioni specifiche:

*Verifica preliminare* - I titolari dei trattamenti devono sottoporre alla verifica preliminare del Garante i sistemi di videosorveglianza che prevedono una raccolta di immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali oppure con dispositivi che rendono identificabile la voce. Vanno altresì sottoposti alla verifica preliminare anche i casi di videosorveglianza dinamico-preventiva che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi e caratteristiche fisionomiche (ad esempio, riconoscimento facciale).

*Autorizzazioni* - I predetti particolari trattamenti devono essere autorizzati preventivamente dal Garante, anche attraverso autorizzazioni generali, solo quando riguardano dati sensibili o giudiziari, ad esempio in caso di ripresa di persone malate o di detenuti.

*Notificazione* - La notificazione non è necessaria in caso di trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio.

Soggetti preposti e misure di sicurezza - Devono essere indicate per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni.

I responsabili e gli incaricati possono essere anche soggetti esterni alla struttura qualora l'organismo esterno svolga prestazioni strumentali e subordinate alle scelte del titolare del trattamento.

**Sanzioni** - La mancata osservanza delle prescrizioni contenute nel provvedimento in esame comporta la illiceità o la non correttezza del trattamento dei dati ed espone alle seguenti sanzioni:

- inutilizzabilità dei dati personali trattati;
- adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- applicazione delle pertinenti sanzioni amministrative o penali.

**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. 5/2004 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<sup>9</sup> stabilisce che i gestori di strutture ricettive non possono dare alloggio a persone sfornite di documento di riconoscimento. Inoltre, i gestori sono tenuti a consegnare ai clienti una scheda di dichiarazione delle generalità, su cui va riportato il nome e cognome, la data ed il luogo di nascita, l'indirizzo e gli estremi del documento di riconoscimento di ciascun cliente.

Tali schede, sottoscritte dal cliente, vanno consegnate a cura del gestore della struttura ricettiva all'autorità locale di pubblica sicurezza. Al posto della consegna manuale, è consentito al gestore inviare alle Questure i dati relativi ai clienti attraverso mezzi informatici.

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

**P'informativa** - All'atto della compilazione della scheda, va data una corretta informativa all'interessato. L'informativa può essere data oralmente o per iscritto, eventualmente utilizzando un cartello da affiggere alla reception della struttura.

**il consenso** – Non è necessario acquisire il consenso dell'interessato, 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.

**P'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.

---

<sup>9</sup> Approvato con RD 18 giugno 1931, n.773.

**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.

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

**P'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** – E' necessario acquisire il consenso, preferibilmente per iscritto, dell'interessato.

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

**P'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.

## **servizio di ricevimento e portineria**

Subito dopo l'entrata in vigore della legge 675 del 1996, ora abrogata dal nuovo Codice della privacy, il Garante, con un comunicato stampa di poche righe, affermò che non sarebbe stato più possibile acquisire informazioni sulla presenza in albergo di un soggetto senza “il consenso diretto dell'interessato a divulgare l'informazione a terzi”.

Così come in altre occasioni, pertanto, il Garante ha voluto interpretare la normativa in senso molto restrittivo, penalizzando le aziende nell'esecuzione di quegli adempimenti che sono comunque conseguenza secondaria di un'obbligazione contrattuale.

Nel contratto di alloggio, infatti, si fornisce ospitalità in una struttura debitamente autorizzata e classificata da enti pubblici locali sulla base di leggi regionali che stabiliscono i requisiti minimi indispensabili per ciascuna categoria. Tra i requisiti obbligatori nella maggioranza delle strutture ricettive c'è anche il servizio di ricevimento e portineria, così come, ad esempio, la pulizia giornaliera delle camere.

Pertanto, il consenso del cliente ad usufruire dei servizi accessori forniti dalla struttura ricettiva (il consenso a ricevere telefonate o messaggi, così come il consenso a far entrare in camera il personale addetto alle pulizie), se previsti come obbligatori dalle leggi regionali di classificazione, dovrebbe considerarsi sempre implicito. Ferma restando, ovviamente, la possibilità per il cliente di rinunciare a questi servizi semplicemente manifestando a coloro che vi sono preposti la volontà di non usufruirne.

L'interpretazione restrittiva del Garante, per fortuna limitata a quei servizi che rendono possibile sapere “se una persona è ospite di un hotel”, nonché la gravità delle sanzioni, impongono pertanto al gestore di una struttura ricettiva alcune cautele.

Pertanto, 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:

**P'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** – Secondo il Garante, è necessario acquisire il consenso dell'interessato. E' anche opportuno che venga acquisito per iscritto.

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

**P'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.

## **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:

**P'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** – 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 l'adesione a sindacati, eccetera).

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

**l'autorizzazione del Garante** – Con l'autorizzazione generale n. 1/2004, 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.

## **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.

## **trattamento dei dati relativi ad agenzie di viaggi o tour operator**

Per i trattamenti di dati personali relativi ad agenzie di viaggi o tour operator, 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 degli interessati.

**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.

## I FACSIMILI



## **l'articolo 7**

Il testo dell'articolo 7 del Codice sulla privacy, contenente i diritti degli interessati al trattamento, 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.*

## il trattamento dei dati dei clienti

### 1- Facsimile di informativa al cliente, da far visionare all'arrivo o da affiggere nella Hall o nelle camere.

Gentile Cliente,  
desideriamo informarLa, ai sensi dell'articolo 7 del Codice sulla privacy (D. Legisl. 196/2003), che il trattamento dei dati personali Suoi e della Sua famiglia riportati nella "scheda di dichiarazione delle generalità degli alloggiati" sarà improntato ai principi di correttezza, liceità e trasparenza e tutelando la Sua riservatezza ed i Suoi diritti. Tale trattamento sarà effettuato anche con l'ausilio di mezzi informatici (senza 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 registrare e comunicare all'autorità locale di pubblica sicurezza le generalità dei clienti alloggiati;
2. per adempiere ai vigenti obblighi contabili e fiscali;
3. per espletare la funzione di ricevimento di messaggi e telefonate a Lei o alla Sua famiglia indirizzati;
4. per inviare al Suo domicilio periodica documentazione sugli aggiornamenti delle tariffe e delle offerte da noi praticate.

Desideriamo inoltre informarLa che il conferimento delle generalità Sue e della Sua famiglia è obbligatorio, ed il Suo eventuale rifiuto a fornirle comporterà per noi l'impossibilità ad ospitarLa nel nostro albergo.

Potrà invece opporsi al trattamento effettuato per le finalità riportate ai punti 3 e 4, semplicemente rivolgendosi a \_\_\_\_\_, Titolare del trattamento (o eventualmente a \_\_\_\_\_, Responsabile del trattamento).

**2- Facsimile alternativo di informativa al cliente completo di formula di consenso, da riportare su un apposito foglio da far sottoscrivere al cliente.** Tale facsimile, debitamente firmato dal cliente, ha il vantaggio di fornire all'albergo la prova documentata che il cliente ha ricevuto una corretta informativa ed ha acconsentito ai trattamenti ulteriori rispetto a quelli obbligatori per legge.

Gentile Cliente,

desideriamo informarLa, ai sensi dell'articolo 7 del Codice sulla privacy (D. Legisl. 196/2003), che il trattamento dei dati personali Suoi e della Sua famiglia, riportati nella "scheda di dichiarazione delle generalità degli alloggiati" sarà improntato ai principi di correttezza, liceità e trasparenza e tutelando la Sua riservatezza ed i Suoi diritti.

Tale trattamento sarà effettuato *anche con l'ausilio di mezzi informatici (senza 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 registrare e comunicare all'autorità locale di pubblica sicurezza le generalità dei clienti alloggiati;
2. per adempiere ai vigenti obblighi contabili e fiscali;
3. per espletare la funzione di ricevimento di messaggi e telefonate a Lei o alla Sua famiglia indirizzati;
4. per inviare al Suo domicilio periodica documentazione sugli aggiornamenti delle tariffe e delle offerte da noi praticate.

Desideriamo inoltre informarLa che il conferimento delle generalità Sue e della Sua famiglia è obbligatorio, ed il Suo eventuale rifiuto a fornirle comporterà per noi l'impossibilità ad ospitarLa nel nostro albergo.

Dovrà invece fornirci il Suo consenso per il trattamento effettuato per le finalità riportate ai punti 3 e 4, sottoscrivendo la dichiarazione sotto riportata.

Per qualsiasi ulteriore informazione potrà rivolgersi a \_\_\_\_\_, Titolare del trattamento (o eventualmente a \_\_\_\_\_, Responsabile del trattamento).

Ai sensi del Codice sulla privacy (D. Legisl. 196/2003), ricevuta l'informativa sul trattamento dei dati personali miei e della mia famiglia:

- autorizzo / non autorizzo l'albergo ad inviare al mio domicilio periodica documentazione sugli aggiornamenti delle tariffe e delle offerte praticate;
- autorizzo / non autorizzo l'albergo alla comunicazione esterna di dati relativi al soggiorno mio e della mia famiglia, al fine esclusivo di consentire la funzione di ricevimento di messaggi e telefonate a noi indirizzati.

Luogo e data.....

Nome, cognome e firma.....

**3- Facsimile alternativo di acquisizione di consenso da riportare eventualmente sulla copia che rimane in albergo della scheda di polizia, per documentare che il cliente ha acconsentito ai trattamenti ulteriori rispetto a quelli obbligatori per legge.** La formula presuppone una informativa orale (o scritta, utilizzando il facsimile riportato al punto1) sulle modalità e finalità del trattamento e presuppone che i dati identificativi del cliente (nome e cognome, indirizzo, ecc.) siano già riportati sulla stessa scheda.

Ai sensi del Codice sulla privacy (D. Legisl 196/2003), ricevuta l'informativa sul trattamento dei dati personali miei e della mia famiglia:

- autorizzo / non autorizzo l'albergo ad inviare al mio domicilio periodica documentazione sugli aggiornamenti delle tariffe e delle offerte praticate;
- autorizzo / non autorizzo l'albergo alla comunicazione esterna di dati relativi al soggiorno mio e della mia famiglia, al fine esclusivo di consentire la funzione di ricevimento di messaggi e telefonate a noi indirizzati.

Firma\_\_\_\_\_.

## **P'informativa e P'acquisizione del consenso per il trattamento dei dati dei lavoratori**

Il facsimile che segue, debitamente adattato, consente di fornire una corretta informativa ai lavoratori in relazione al trattamento dei loro dati. Il facsimile è integrato dalla formula per l'acquisizione del consenso scritto, indispensabile qualora vengano trattati dati sensibili:

### **Informativa**

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, 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, il trattamento è effettuato, su nostro incarico, dal Sig. \_\_\_\_\_, 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 \_\_\_\_\_).

**Formula di consenso per il trattamento di dati personali sensibili**

Acquisite le informazioni relative al trattamento dei miei dati personali sensibili ai sensi dell'articolo 13 del Codice sulla privacy (Decreto Legislativo 196/2003), acconsento al loro trattamento 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 del codice identificativo personale e della chiave di accesso**

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" 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 delle generalità dei clienti alloggiati, da loro stessi riportate nelle schede di polizia o rilevate dai documenti di riconoscimento da loro esibiti, effettuata in adempimento della normativa di polizia vigente (art. 109 Testo Unico delle leggi di polizia);
- notifica delle suddette generalità agli uffici di polizia competenti, attraverso la consegna giornaliera delle schede di polizia sottoscritte dai clienti (in alternativa: attraverso l'invio telematico dei suddetti dati debitamente autorizzato dalla Questura competente);
- 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 liceità, l'incaricato si avvarrà dell'ausilio di strumenti elettronici, e pertanto viene conferita la seguente PAROLA CHIAVE \_\_\_\_\_ ed il seguente CODICE IDENTIFICATIVO PERSONALE \_\_\_\_\_.

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

La parola chiave, 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 sottoscritto \_\_\_\_\_ titolare / responsabile dei trattamenti di dati personali, conferisce al Sig. \_\_\_\_\_ l'incarico di custodire le copie delle credenziali di autenticazione attribuite ai soggetti incaricati del trattamento di dati personali effettuato con l'ausilio di strumenti elettronici.

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

Data e firma del sottoscritto

Firma dell'incaricato per ricevuta

## **il documento programmatico sulla sicurezza**

Il modello che segue, opportunamente verificato ed integrato secondo le peculiarità dell'organizzazione del lavoro e tecnica della azienda, può essere utilizzato per la redazione del DPS.

Ricordiamo che la redazione del DPS è obbligatoria per le aziende ricettive solo nel caso di trattamenti di dati sensibili con l'ausilio di strumenti elettronici. La redazione del documento programmatico sulla sicurezza non è invece necessaria in caso di trattamenti di dati sensibili effettuato in forma cartacea.

Il DPS dovrà essere redatto annualmente (entro il 31 marzo) e di esso dovrà farsi menzione nella relazione accompagnatoria del bilancio d'esercizio.

In via transitoria, il DPS dovrà essere realizzato per la prima volta entro il 31 dicembre 2004.

## DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Dati dell'azienda: \_\_\_\_\_

Titolare dei trattamenti: \_\_\_\_\_

Responsabile dei trattamenti: \_\_\_\_\_

### ELENCO DEI TRATTAMENTI DI DATI PERSONALI SENSIBILI E LORO DESCRIZIONE SINTETICA - esempio:

**codice identificativo A:** Trattamento dei dati sensibili dei lavoratori concernenti la fruizione di permessi e festività religiose o di servizi particolari di mensa, nonché relativi alla manifestazione dell'obiezione di coscienza.

**codice identificativo B:** Trattamento dei dati sensibili dei lavoratori effettuato ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali, concernenti l'esercizio di funzioni pubbliche e di incarichi politici, di attività o di incarichi sindacali, 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.

**codice identificativo C:** Trattamento dei dati sensibili dei lavoratori 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.

**codice identificativo D:** Trattamento dei dati sensibili dei clienti disabili, o richiedenti servizi particolari in relazione allo stato di salute, ad un credo religioso, o all'orientamento sessuale.

**DESCRIZIONE DEGLI STRUMENTI UTILIZZATI -  
esempio:**

**Codice A:** Data base applicazione Windows.

**Ubicazione fisica dei supporti di memorizzazione:** Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo via\_\_\_\_\_.

**Tipologia di dispositivi di accesso:** pc n.\_\_\_\_\_.

**Tipologia di interconnessione:** Rete locale LAN.

**Codice B:** Data base applicazione Windows.

**Ubicazione fisica dei supporti di memorizzazione:** Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo via\_\_\_\_\_.

**Tipologia di dispositivi di accesso:** pc n.\_\_\_\_\_.

**Tipologia di interconnessione:** Rete locale LAN.

**Codice C:** Data base applicazione Windows.

**Ubicazione fisica dei supporti di memorizzazione:** Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo via\_\_\_\_\_.

**Tipologia di dispositivi di accesso:** pc n.\_\_\_\_\_.

**Tipologia di interconnessione:** Rete locale LAN.

**Codice D:** Data base applicazione Windows.

**Ubicazione fisica dei supporti di memorizzazione:** Hard disk su pc server ubicato presso la struttura ricettiva, indirizzo via\_\_\_\_\_.

**Tipologia di dispositivi di accesso:** pc n.\_\_\_\_\_.

**Tipologia di interconnessione:** Rete locale LAN.

## **STRUTTURE PREPOSTE AI TRATTAMENTI - esempio:**

**Reparto:** Ricevimento

**Trattamenti effettuati:** Codice D

**Compiti e responsabilità:** Acquisizione, caricamento e consultazione dati.

**Reparto:** Amministrazione

**Trattamenti effettuati:** Codici A, B, C, D

**Compiti e responsabilità:** Acquisizione, caricamento e consultazione dati. Comunicazione a terzi solo se previsto da obblighi di legge o consentito dagli interessati.

**Reparto:** Ufficio del personale

**Trattamenti effettuati:** Codici A, B, C

**Compiti e responsabilità:** Acquisizione, caricamento e consultazione dati. Comunicazione a terzi solo se previsto da obblighi di legge o consentito dagli interessati.

## **ANALISI DEI RISCHI CHE INCOMBONO SUI DATI - esempio:**

### **Comportamento degli operatori**

**Furto di credenziali di autenticazione** (password e user-id): l'accesso alla struttura ricettiva, e dunque agli elaboratori ed al database, è continuamente sorvegliato e quindi è altamente improbabile che l'eventuale sottrazione delle credenziali di autenticazione possa procurare esiti dannosi. Il sistema, comunque, mantiene traccia degli accessi praticati allo scopo di accertare eventuali comportamenti illegittimi. Rischio basso.

**Carenza di consapevolezza, disattenzione o incuria:** La consapevolezza del personale, conseguente al livello professionale dello stesso ed alle disposizioni adottate in materia di privacy, rende altamente improbabile comportamenti di disattenzione o incuria da parte dei dipendenti. Rischio basso.

**Comportamenti sleali o fraudolenti:** L'obbligo di lealtà implicito nei rapporti di lavoro rende mediamente improbabile comportamenti

sleali e fraudolenti finalizzati ad un uso improprio dei dati. Rischio medio.

**Errore materiale:** L'utilizzo di procedure automatizzate e la competenza e professionalità dei lavoratori rendono mediamente improbabile il verificarsi di errori materiali. Rischio medio.

#### Eventi relativi agli strumenti

**Azione di virus informatici o di codici malefici:** Il sistema è protetto da un dispositivo Firewall che aggiorna anche periodicamente i pattern di verifica antivirus. Su ogni stazione è installato il relativo filtro antivirus. Nel caso in cui dovesse comunque verificarsi l'evento, gli archivi possono essere immediatamente ripristinati poiché viene effettuato backup giornaliero in duplice copia degli archivi stessi. Rischio basso.

**Spamming o altre tecniche di sabotaggio:** Il dispositivo Firewall protegge anche da programmi in grado di generare in seguito spamming. Rischio basso.

**Malfunzionamento, indisponibilità o degrado degli strumenti:** Il controllo sullo stato dell'hardware è costante e le eventuali operazioni di ripristino possono essere effettuate in tempi brevi. Guasti e malfunzionamenti non possono però essere completamente esclusi. Rischio basso.

**Accessi esterni non autorizzati:** Attraverso Internet l'accesso è impedito dal dispositivo Firewall. Rischio basso.

**Intercettazione di informazioni in rete:** I dati sono protetti da password. Rischio basso.

#### Eventi relativi al contesto

**Accessi non autorizzati a locali/reparti ad accesso ristretto; asportazione e furto di strumenti contenenti dati:** L'accesso alla struttura ricettiva è continuamente presidiato. Rischio basso.

**Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria:** Tali eventi non possono essere totalmente esclusi, anche se la struttura è tenuta al rispetto di precise regole di sicurezza e prevenzione incendi. Le eventuali operazioni di ripristino possono essere però effettuate in tempi brevi. Rischio basso.

**Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.):** L'impianto elettrico è costantemente

mantenuto ed è presente il gruppo di continuità. Rischio basso.

**Errori umani nella gestione della sicurezza fisica:** Il personale è adeguatamente formato in ordine alla prevenzione di rischi. Rischio basso.

#### MISURE ADOTTATE E DA ADOTTARE - esempio

**Adeguate informazione del personale relativamente alle disposizioni della normativa vigente in materia di privacy:**

Misura adottata

**Rischi contrastati:** derivanti dal comportamento degli operatori.

**Trattamenti interessati:** Codici A, B, C, D.

**Struttura o persone addette all'adozione:** Direzione.

**Predisposizione di istruzioni e comunicazione di direttive vincolanti, a mezzo ordine di servizio, relative ai comportamenti operativi che ciascun incaricato al trattamento deve adottare in ottemperanza alla normativa vigente:**

Misura adottata

**Rischi contrastati:** derivanti dal comportamento degli operatori.

**Trattamenti interessati:** Codici A, B, C, D.

**Struttura o persone addette all'adozione:** Direzione.

**Utilizzo delle "credenziali di autenticazione" aventi le caratteristiche e le modalità operative prescritte dal Codice sulla privacy :**

Misura adottata

**Rischi contrastati:** eventi relativi agli strumenti.

**Trattamenti interessati:** Codici A, B, C, D.

**Struttura o persone addette all'adozione:** Società di consulenza informatica, su disposizioni della Direzione.

**Installazione di idonei strumenti elettronici e programmi atti a proteggere i dati da intrusioni, accesso abusivo o danneggiamenti di virus o programmi esterni, nel rispetto di quanto stabilito dal Codice sulla privacy:**

Misura adottata

**Rischi contrastati:** eventi relativi agli strumenti.

**Trattamenti interessati:** Codici A, B, C, D.

**Struttura o persone addette all'adozione:** Società di consulenza

informatica, su disposizioni della Direzione.

**Aggiornamento almeno semestrale dei programmi atti a prevenire la vulnerabilità degli elaboratori e a correggerne eventuali difetti:** Misura adottata

**Rischi contrastati:** eventi relativi agli strumenti.

**Trattamenti interessati:** Codici A, B, C, D.

**Struttura o persone addette all'adozione:** Società di consulenza informatica, su disposizioni della Direzione.

**Divieto posto in capo agli operatori di consentire l'accesso a persone non autorizzate all'interno dei locali ove sono custoditi i dati:** Misura adottata

**Rischi contrastati:** eventi relativi al contesto.

**Trattamenti interessati:** Codici A, B, C, D.

**Struttura o persone addette all'adozione:** addetti al ricevimento e portieri, nonché addetti all'amministrazione e all'ufficio del personale, su disposizioni della Direzione.

**Controllo periodico e manutenzione degli impianti elettrici e dei sistemi complementari:** Misura adottata

**Rischi contrastati:** eventi relativi al contesto.

**Trattamenti interessati:** Codici A, B, C, D.

**Struttura o persone addette all'adozione:** personale tecnico competente, su disposizioni della Direzione.

#### **CRITERI E PROCEDURE PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI – esempio:**

**Banca dati/Data base/Archivio:** Data base anagrafiche clienti e prestazioni.

**Criteri e procedure per il salvataggio ed il ripristino dei dati:** Sistema di backup su nastro centralizzato, situato sul server.

**Pianificazione delle prove di ripristino:** Il sistema di backup verifica i dati copiati alla fine di ogni operazione eseguita. Di fatto la pianificazione è giornaliera.

**Banca dati/Data base/Archivio:** Data base anagrafiche personale.

**Criteri e procedure per il salvataggio ed il ripristino dei dati:**

Sistema di backup su nastro centralizzato, situato sul server.

**Pianificazione delle prove di ripristino:** Il sistema di backup verifica i dati copiati alla fine di ogni operazione eseguita. Di fatto la pianificazione è giornaliera.

## **PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI – esempio:**

**Descrizione sintetica degli interventi formativi previsti:** Il personale incaricato è stato puntualmente informato in merito alle disposizioni normative in materia di privacy ed alla corretta esecuzione delle direttive impartite in materia con specifico ordine di servizio.

**Classi di incarico o tipologie di incaricati interessati:** Tutti i dipendenti incaricati di trattamenti di dati personali.

**Tempi previsti:** Già effettuato.

**Descrizione sintetica degli interventi formativi previsti:** Il personale incaricato sarà aggiornato periodicamente sull'evoluzione della normativa e sulle possibilità di migliorare e ottimizzare le misure di protezione adottate.

**Classi di incarico o tipologie di incaricati interessati:** Tutti i dipendenti incaricati di trattamenti di dati personali.

**Tempi previsti:** Incontri semestrali.

**Descrizione sintetica degli interventi formativi previsti:** Il personale incaricato è stato istruito dal consulente informatico sul corretto utilizzo delle “credenziali di autenticazione” e delle misure tecniche adottate per la sicurezza dei dati.

**Classi di incarico o tipologie di incaricati interessati:** Tutti i dipendenti incaricati di trattamenti di dati personali.

**Tempi previsti:** Già effettuato. Sono previsti aggiornamenti periodici.

## **TRATTAMENTI AFFIDATI ALL'ESTERNO – esempio:**

**Descrizione sintetica dell'attività esternalizzata:** Consulenza, gestione tecnica e aggiornamento dei sistemi informatici (hardware e software).

**Trattamento di dati interessato:** Codici A, B, C, D.

**Soggetto esterno:** Società \_\_\_\_\_ con sede in\_\_\_\_\_.

**Descrizione dei criteri e degli impegni assunti per l'adozione delle misure:** La società incaricata ha assicurato l'adempimento degli obblighi previsti dal Codice sulla privacy ed ha fornito il nominativo del funzionario responsabile per la privacy. Si è impegnata ad effettuare il trattamento al solo fine di espletare gli incarichi ricevuti in virtù dell'attività professionale e di consulenza prestata. Si è infine impegnata a rilasciare dettagliate relazioni periodiche contenenti la descrizione dei dispositivi di sicurezza adottati e attestanti la conformità del sistema elettronico ed informatico alle disposizioni normative vigenti.

**Descrizione sintetica dell'attività esternalizzata:** Consulenza in materia di disciplina del lavoro ed elaborazione delle buste paga.

**Trattamento di dati interessato:** Codici A, B, C.

**Soggetto esterno:** Società \_\_\_\_\_ con sede in\_\_\_\_\_.

**Descrizione dei criteri e degli impegni assunti per l'adozione delle misure:** La società incaricata ha assicurato l'adempimento degli obblighi previsti dal Codice sulla privacy ed ha fornito il nominativo del funzionario responsabile per la privacy. Si è impegnata ad effettuare il trattamento al solo fine di espletare gli incarichi ricevuti in virtù dell'attività professionale e di consulenza prestata. Si è infine impegnata a rilasciare dettagliate relazioni periodiche contenenti la descrizione dei dispositivi di sicurezza adottati e attestanti la conformità del sistema elettronico ed informatico alle disposizioni normative vigenti.

## **GLI ALLEGATI**



## **il decreto legislativo 30 giugno 2003 n. 196 (stralcio)**

### **DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196 - CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**

*Vigenza 27 febbraio 2004 – Consolidato con la legge 26 febbraio 2004, n. 45 di conversione con modifiche dell'art. 3 del d.l. 24 dicembre 2003, n. 354.*

#### **IL PRESIDENTE DELLA REPUBBLICA**

VISTI gli articoli 76 e 87 della Costituzione;

VISTO l'articolo 1 della legge 24 marzo 2001, n. 127, recante delega a Governo per l'emanazione di un testo unico in materia di trattamento dei dati personali;

VISTO l'articolo 26 della legge 3 febbraio 2003, n. 14, recante disposizioni per l'adempimento di obblighi derivanti all'appartenenza dell'Italia alle Comunità europee (legge comunitaria 2002);

VISTA la legge 31 dicembre 1996, n. 675, e successive modificazioni;

VISTA la legge 31 dicembre 1996, n. 676, recante delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

VISTA la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati;

VISTA la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;

VISTA la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 9 maggio 2003;

SENTITO il Garante per la protezione dei dati personali;

ACQUISITO il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

VISTA la deliberazione del Consiglio dei Ministri, adottata nella riunione del 27 giugno 2003;

SULLA PROPOSTA del Presidente del Consiglio dei Ministri, del Ministro per la funzione pubblica e del Ministro per le politiche comunitarie, di concerto con i Ministri della giustizia, dell'economia e delle finanze, degli affari esteri e delle comunicazioni;

EMANA il seguente decreto legislativo:

#### **PARTE I - DISPOSIZIONI GENERALI**

##### **Titolo I - PRINCIPI GENERALI**

###### **Art. 1. Diritto alla protezione dei dati personali**

1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

### **Art. 2. Finalità**

1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

### **Art. 3. Principio di necessità nel trattamento dei dati**

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

### **Art. 4. Definizioni**

1. Ai fini del presente codice si intende per:

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti 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 di dati;

b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "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;

e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, 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 ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) "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;

g) "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;

h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) "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;

m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) "chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) "abbonato", qualunque persona fisica, persona giuridica, ente o associazione parte

di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) "dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) "servizio a valore aggiunto", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:

a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) "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;

e) "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;

f) "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;

g) "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.

4. Ai fini del presente codice si intende per:

a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

#### **Art. 5. Oggetto ed ambito di applicazione**

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.

#### **Art. 6. Disciplina del trattamento**

1. Le disposizioni contenute nella presente Parte si applicano a tutti i trattamenti di dati, salvo quanto previsto, in relazione ad alcuni trattamenti, dalle disposizioni integrative o modificative della Parte II.

### **Titolo II - DIRITTI DELL'INTERESSATO**

#### **Art. 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, ancorchè 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.

#### **Art. 8. Esercizio dei diritti**

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:

- a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
- b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
- c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
- d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonchè alla tutela della loro stabilità;
- e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
- f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
- g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
- h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1 aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f) provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonchè l'indicazione di condotte da tenersi o di decisioni in via di

assunzione da parte del titolare del trattamento.

#### **Art. 9. Modalità di esercizio**

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.
2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.
3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.
5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

#### **Art. 10. Riscontro all'interessato**

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
  - a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
  - b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.
2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.
3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.
4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla

richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

### **Titolo III - REGOLE GENERALI PER IL TRATTAMENTO DEI DATI CAPO I - REGOLE PER TUTTI I TRATTAMENTI**

#### **Art. 11. Modalità del trattamento e requisiti dei dati**

1. I dati personali oggetto di trattamento sono:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento intermini 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.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

### **Art. 12. Codici di deontologia e di buona condotta**

1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.
2. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice.
3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.
4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

### **Art. 13. Informativa**

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
  - a) le finalità e le modalità del trattamento cui sono destinati i dati;
  - b) la natura obbligatoria o facoltativa del conferimento dei dati;
  - c) le conseguenze di un eventuale rifiuto di rispondere;
  - d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
  - e) i diritti di cui all'articolo 7;
  - f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.
2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.
3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.
4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non

oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:

- a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, 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;
- c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

#### **Art. 14. Definizione di profili e della personalità dell'interessato**

1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

2. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17.

#### **Art. 15. Danni cagionati per effetto del trattamento**

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

#### **Art. 16. Cessazione del trattamento**

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

- a) distrutti;
- b) ceduti ad altro titolare, purchè destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
- c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
- d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

2. La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

#### **Art. 17. Trattamento che presenta rischi specifici**

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonchè per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può

determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

## **CAPO II - REGOLE ULTERIORI PER I SOGGETTI PUBBLICI**

### **Art. 18. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici**

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.

2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonchè dalla legge e dai regolamenti.

4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.

5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

### **Art. 19. Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari**

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.

3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

### **Art. 20. Principi applicabili al trattamento di dati sensibili**

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici

a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.

3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.

4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente

#### **Art. 21. Principi applicabili al trattamento di dati giudiziari**

1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.

#### **Art. 22. Principi applicabili al trattamento di dati sensibili e giudiziari**

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante

l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

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

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

### **CAPO III - REGOLE ULTERIORI PER PRIVATI ED ENTI PUBBLICI ECONOMICI**

#### **Art. 23. Consenso**

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

#### **Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso**

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

- b) 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;
- c) 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;
- d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;
- f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, 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, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;
- h) 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;
- i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

#### **Art. 25. Divieti di comunicazione e diffusione**

1. La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria:

- a) in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e);
- b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.

2. è fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

#### **Art. 26. Garanzie per i dati sensibili**

1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

3. Il comma 1 non si applica al trattamento:

a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

b) dei 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.

4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n.397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i

dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto 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;

d) quando 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, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

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

#### **Art. 27. Garanzie per i dati giudiziari**

1. Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specificchino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

### **TITOLO IV - SOGGETTI CHE EFFETTUANO IL TRATTAMENTO**

#### **Art. 28. Titolare del trattamento**

1. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

#### **Art. 29. Responsabile del trattamento**

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

#### **Art. 30. Incaricati del trattamento**

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera 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.

**Titolo V - SICUREZZA DEI DATI E DEI SISTEMI**  
**CAPO I - MISURE DI SICUREZZA**

**Art. 31. Obblighi di sicurezza**

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

**Art. 32. Particolari titolari**

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

**CAPO II - MISURE MINIME DI SICUREZZA**

**Art. 33. Misure minime**

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

**Art. 34. Trattamenti con strumenti elettronici**

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) autenticazione informatica;
- b) adozione di procedure di gestione delle credenziali di autenticazione;

- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza;
- h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

#### **Art. 35. Trattamenti senza l'ausilio di strumenti elettronici**

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

#### **Art. 36. Adeguamento**

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

### **Titolo VI - ADEMPIMENTI**

#### **Art. 37. Notificazione del trattamento**

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:

- a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- b) 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 diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
- c) 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;

- d) 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;
  - e) 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;
  - f) 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.
2. Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla Gazzetta ufficiale della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.
3. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.
4. Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

### **Art. 38. Modalità di notificazione**

1. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.
2. La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione.
3. Il Garante favorisce la disponibilità del modello per via telematica e la notificazione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.
4. Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.
5. Il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente.
6. Il titolare del trattamento che non è tenuto alla notificazione al Garante ai sensi dell'articolo 37 fornisce le notizie contenute nel modello di cui al comma 2 a chi ne fa richiesta, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

**Art. 39. Obblighi di comunicazione**

1. Il titolare del trattamento è tenuto a comunicare previamente al Garante le seguenti circostanze:

a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;

b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo.

2. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante.

3. La comunicazione di cui al comma 1 è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa a quest'ultimo per via telematica osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento di cui all'articolo 38, comma 2, oppure mediante telefax o lettera raccomandata.

**Art. 40. Autorizzazioni generali**

1. Le disposizioni del presente codice che prevedono un'autorizzazione del Garante sono applicate anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate nella Gazzetta Ufficiale della Repubblica italiana.

**Art. 41. Richieste di autorizzazione**

1. Il titolare del trattamento che rientra nell'ambito di applicazione di un'autorizzazione rilasciata ai sensi dell'articolo 40 non è tenuto a presentare al Garante una richiesta di autorizzazione se il trattamento che intende effettuare è conforme alle relative prescrizioni.

2. Se una richiesta di autorizzazione riguarda un trattamento autorizzato ai sensi dell'articolo 40 il Garante può provvedere comunque sulla richiesta se le specifiche modalità del trattamento lo giustificano.

3. L'eventuale richiesta di autorizzazione è formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante e trasmessa a quest'ultimo per via telematica, osservando le modalità di sottoscrizione e conferma del ricevimento di cui all'articolo 38, comma 2. La medesima richiesta e l'autorizzazione possono essere trasmesse anche mediante telefax o lettera raccomandata.

4. Se il richiedente è invitato dal Garante a fornire informazioni o ad esibire documenti, il termine di quarantacinque giorni di cui all'articolo 26, comma 2, decorre dalla data di scadenza del termine fissato per l'adempimento richiesto.

5. In presenza di particolari circostanze, il Garante può rilasciare un'autorizzazione provvisoria a tempo determinato.

## TITOLO VII - TRASFERIMENTO DEI DATI ALL'ESTERO

### **Art. 42. Trasferimenti all'interno dell'Unione europea**

1. Le disposizioni del presente codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

### **Art. 43. Trasferimenti consentiti in Paesi terzi**

1. Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito quando:

- a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta;
- b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;
- c) è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21;
- d) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;
- e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
- f) è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;
- g) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;
- h) il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

#### **Art. 44. Altri trasferimenti consentiti**

1. Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:

- a) individuate dal Garante anche in relazione a garanzie prestate con un contratto;
- b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

#### **Art. 45. Trasferimenti vietati**

1. Fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

### **TITOLO VIII - LAVORO E PREVIDENZA SOCIALE**

#### **CAPO I - PROFILI GENERALI**

#### **Art. 111. Codice di deontologia e di buona condotta**

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione degli annunci per finalità di occupazione di cui all'articolo 113, comma 3 e alla ricezione di curricula contenenti dati personali anche sensibili.

#### **Art. 112. Finalità di rilevante interesse pubblico**

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato.

2. Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, quelli effettuati al fine di:

- a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette;
- b) garantire le pari opportunità;
- c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal

servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;

d) adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali;

e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale;

f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del decreto legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a tipi di dati individuati specificamente;

g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;

h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;

i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;

l) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;

m) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale;

n) svolgere l'attività di indagine e ispezione presso soggetti pubblici;

o) valutare la qualità dei servizi resi e dei risultati conseguiti.

3. La diffusione dei dati di cui alle lettere m), n) ed o) del comma 2 è consentita in forma anonima e, comunque, tale da non consentire l'individuazione dell'interessato.

## **CAPO II - ANNUNCI DI LAVORO E DATI RIGUARDANTI PRESTATORI DI LAVORO**

### **Art. 113. Raccolta di dati e pertinenza**

1. Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300.

## **CAPO III - DIVIETO DI CONTROLLO A DISTANZA E TELELAVORO**

### **Art. 114. Controllo a distanza**

1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.

**Art. 115. Telelavoro e lavoro a domicilio**

1. Nell'ambito del rapporto di lavoro domestico e del telelavoro il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale.

2. Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

**CAPO IV - ISTITUTI DI PATRONATO E DI ASSISTENZA SOCIALE****Art. 116. Conoscibilità di dati su mandato dell'interessato**

1. Per lo svolgimento delle proprie attività gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato ai sensi dell'articolo 23.

2. Il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le linee-guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni.

**TITOLO X - COMUNICAZIONI ELETTRONICHE****CAPO I - SERVIZI DI COMUNICAZIONE ELETTRONICA****Art. 121. Servizi interessati**

1. Le disposizioni del presente titolo si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni.

**Art. 122. Informazioni raccolte nei riguardi dell'abbonato o dell'utente**

1. Salvo quanto previsto dal comma 2, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

2. Il codice di deontologia di cui all'articolo 133 individua i presupposti e i limiti entro i quali l'uso della rete nei modi di cui al comma 1, per determinati scopi legittimi relativi alla memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il consenso sulla base di una previa informativa ai sensi dell'articolo 13 che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento.

#### **Art. 123. Dati relativi al traffico**

1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.

2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il proprio consenso, che è revocabile in ogni momento.

4. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

5. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

6. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione.

#### **Art. 124. Fatturazione dettagliata**

1. L'abbonato ha diritto di ricevere in dettaglio, a richiesta e senza alcun aggravio di spesa, la dimostrazione degli elementi che compongono la fattura relativi, in particolare, alla data e all'ora di inizio della conversazione, al numero selezionato, al tipo di numerazione, alla località, alla durata e al numero di scatti addebitati per ciascuna conversazione.

2. Il fornitore del servizio di comunicazione elettronica accessibile al pubblico è tenuto 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.

3. Nella documentazione inviata all'abbonato relativa alle comunicazioni effettuate

non sono evidenziati i servizi e le comunicazioni di cui al comma 2, nè le comunicazioni necessarie per attivare le modalità alternative alla fatturazione.

4. Nella fatturazione all'abbonato non sono evidenziate le ultime tre cifre dei numeri chiamati. Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati, l'abbonato può richiedere la comunicazione dei numeri completi delle comunicazioni in questione.

5. Il Garante, accertata l'effettiva disponibilità delle modalità di cui al comma 2, può autorizzare il fornitore ad indicare nella fatturazione i numeri completi delle comunicazioni.

#### **Art. 125. Identificazione della linea**

1. Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'utente chiamante la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea.

2. Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione delle chiamate entranti.

3. Se è disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avviene prima che la comunicazione sia stabilita, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità, mediante una funzione semplice e gratuita, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante.

4. Se è disponibile la presentazione dell'identificazione della linea collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea collegata all'utente chiamante.

5. Le disposizioni di cui al comma 1 si applicano anche alle chiamate dirette verso Paesi non appartenenti all'unione europea. Le disposizioni di cui ai commi 2, 3 e 4 si applicano anche alle chiamate provenienti da tali Paesi.

6. Se è disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e gli utenti dell'esistenza di tale servizio e delle possibilità previste ai commi 1, 2, 3 e 4.

#### **Art. 126. Dati relativi all'ubicazione**

1. I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'abbonato ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto.

2. Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e gli

abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto.

3. L'utente e l'abbonato che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni.

4. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30, sono la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

#### **Art. 127. Chiamate di disturbo e di emergenza**

1. L'abbonato che riceve chiamate di disturbo può richiedere che il fornitore della rete pubblica di comunicazioni o del servizio di comunicazione elettronica accessibile al pubblico renda temporaneamente inefficace la soppressione della presentazione dell'identificazione della linea chiamante e conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione può essere disposta per i soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni.

2. La richiesta formulata per iscritto dall'abbonato specifica le modalità di ricezione delle chiamate di disturbo e nel caso in cui sia preceduta da una richiesta telefonica è inoltrata entro quarantotto ore.

3. I dati conservati ai sensi del comma 1 possono essere comunicati all'abbonato che dichiara di utilizzarli per esclusive finalità di tutela rispetto a chiamate di disturbo. Per i servizi di cui al comma 1 il fornitore assicura procedure trasparenti nei confronti degli abbonati e può richiedere un contributo spese non superiore ai costi effettivamente sopportati.

4. Il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico predispone procedure trasparenti per garantire, linea per linea, l'inefficacia della soppressione dell'identificazione della linea chiamante, nonché, ove necessario, il trattamento dei dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, da parte dei servizi abilitati in base alla legge a ricevere chiamate d'emergenza. I servizi sono individuati con decreto del Ministro delle comunicazioni, sentiti il Garante e l'Autorità per le garanzie nelle comunicazioni.

#### **Art. 128. Trasferimento automatico della chiamata**

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta le misure necessarie per consentire a ciascun abbonato, gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico delle

chiamate verso il proprio terminale effettuato da terzi.

#### **Art. 129. Elenchi di abbonati**

1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 3, e in conformità alla normativa comunitaria, le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico, anche in riferimento ai dati già raccolti prima della data di entrata in vigore del presente codice.

2. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per le finalità di cui all'articolo 7, comma 4, lettera b), in base al principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca dell'abbonato per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri.

#### **Art. 130. Comunicazioni indesiderate**

1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24.

4. Fatto salvo quanto previsto nel comma 1, 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 e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. È vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7.

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

**Art. 131. Informazioni ad abbonati e utenti**

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa l'abbonato e, ove possibile, l'utente circa la sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei.
2. L'abbonato informa l'utente quando il contenuto delle comunicazioni o conversazioni può essere appreso da altri a causa del tipo di apparecchiature terminali utilizzate o del collegamento realizzato tra le stesse presso la sede dell'abbonato medesimo.
3. L'utente informa l'altro utente quando, nel corso della conversazione, sono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti.

**Art. 132. Conservazione di dati di traffico per altre finalità**

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi, per finalità di accertamento e repressione di reati.
2. Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico sono conservati dal fornitore per ulteriori ventiquattro mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.
3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del giudice su istanza del pubblico ministero o del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-quater del codice di procedura penale.
4. Dopo la scadenza del termine indicato al comma 1, il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi dei delitti di cui all'articolo 407, comma 2, lettera a), del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.
5. Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti anche a:
  - a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'Allegato B);
  - b) disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;
  - c) individuare le modalità di trattamento dei dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, l'utilizzazione dei dati sia consentita solo nei casi di cui al comma 4 e all'articolo 7;
  - d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2.

## **CAPO II - INTERNET E RETI TELEMATICHE**

### **Art. 133. Codice di deontologia e di buona condotta**

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica, con particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di comunicazione elettronica gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole e interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 11, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato.

## **CAPO III - VIDEOSORVEGLIANZA**

### **Art. 134. Codice di deontologia e di buona condotta**

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11.

## **TITOLO XIII - MARKETING DIRETTO**

### **CAPO I - PROFILI GENERALI**

#### **Art. 140. Codice di deontologia e di buona condotta**

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale, prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni.

## PARTE III - TUTELA DELL'INTERESSATO E SANZIONI

### TITOLO I - TUTELA AMMINISTRATIVA E GIURISDIZIONALE

#### CAPO I - TUTELA DINANZI AL GARANTE

##### SEZIONE I - PRINCIPI GENERALI

###### **Art. 141. Forme di tutela**

1. L'interessato può rivolgersi al Garante:

- a) mediante reclamo circostanziato nei modi previsti dall'articolo 142, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
- b) mediante segnalazione, se non è possibile presentare un reclamo circostanziato ai sensi della lettera a), al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
- c) mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 secondo le modalità e per conseguire gli effetti previsti nella sezione III del presente capo.

##### SEZIONE II - TUTELA AMMINISTRATIVA

###### **Art. 142. Proposizione dei reclami**

1. Il reclamo contiene 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 dell'istante.
2. Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano anche ai sensi dell'articolo 9, comma 2, ed è presentato al Garante senza particolari formalità. Il reclamo reca in allegato la documentazione utile al fine della sua valutazione e l'eventuale procura, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.
3. Il Garante può predisporre un modello per il reclamo da pubblicare nel Bollettino e di cui favorisce la disponibilità con strumenti elettronici.

###### **Art. 143. Procedimento per i reclami**

1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento:
  - a) prima di prescrivere le misure di cui alla lettera b), ovvero il divieto o il blocco ai sensi della lettera c), può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente;
  - b) prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;

c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), 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;

d) 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.

2. I provvedimenti di cui al comma 1 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.

#### **Art. 144. Segnalazioni**

1. I provvedimenti di cui all'articolo 143 possono essere adottati anche a seguito delle segnalazioni di cui all'articolo 141, comma 1, lettera b), se è avviata un'istruttoria preliminare e anche prima della definizione del procedimento.

### **SEZIONE III - TUTELA ALTERNATIVA A QUELLA GIURISDIZIONALE**

#### **Art. 145. Ricorsi**

1. I diritti di cui all'articolo 7 possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante.

2. Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.

3. La presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

#### **Art. 146. Interpello preventivo**

1. Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che è stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile ai sensi dell'articolo 8, comma 1, e sono decorsi i termini previsti dal presente articolo, ovvero è stato opposto alla richiesta un diniego anche parziale.

2. Il riscontro alla richiesta da parte del titolare o del responsabile è fornito entro quindici giorni dal suo ricevimento.

3. Entro il termine di cui al comma 2, 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.

#### **Art. 147. Presentazione del ricorso**

1. Il ricorso è proposto nei confronti del titolare e indica:

a) gli estremi identificativi del ricorrente, dell'eventuale procuratore speciale, del titolare e, ove conosciuto, del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7;

- b) la data della richiesta presentata al titolare o al responsabile ai sensi dell'articolo 8, comma 1, oppure del pregiudizio imminente ed irreparabile che permette di prescindere dalla richiesta medesima;
  - c) gli elementi posti a fondamento della domanda;
  - d) il provvedimento richiesto al Garante; e) il domicilio eletto ai fini del procedimento.
2. Il ricorso è sottoscritto dal ricorrente o dal procuratore speciale e reca in allegato:
- a) la copia della richiesta rivolta al titolare o al responsabile ai sensi dell'articolo 8, comma 1;
  - b) l'eventuale procura;
  - c) la prova del versamento dei diritti di segreteria.
3. Al ricorso è unita, altresì, la documentazione utile ai fini della sua valutazione e l'indicazione di un recapito per l'invio di comunicazioni al ricorrente o al procuratore speciale mediante posta elettronica, telefax o telefono.
4. Il ricorso è rivolto al Garante e la relativa sottoscrizione è autenticata. L'autenticazione non è richiesta se la sottoscrizione è apposta presso l'Ufficio del Garante o da un procuratore speciale iscritto all'albo degli avvocati al quale la procura è conferita ai sensi dell'articolo 83 del codice di procedura civile, ovvero con firma digitale in conformità alla normativa vigente.
5. Il ricorso è validamente proposto solo se è trasmesso con plico raccomandato, oppure per via telematica osservando le modalità relative alla sottoscrizione con firma digitale e alla conferma del ricevimento prescritte ai sensi dell'articolo 38, comma 2, ovvero presentato direttamente presso l'Ufficio del Garante.

#### **Art. 148. Inammissibilità del ricorso**

1. Il ricorso è inammissibile:
- a) se proviene da un soggetto non legittimato;
  - b) in caso di inosservanza delle disposizioni di cui agli articoli 145 e 146;
  - c) se difetta di taluno degli elementi indicati nell'articolo 147, commi 1 e 2, salvo che sia regolarizzato dal ricorrente o dal procuratore speciale anche su invito dell'Ufficio del Garante ai sensi del comma 2, entro sette giorni dalla data della sua presentazione o della ricezione dell'invito. In tale caso, il ricorso si considera presentato al momento in cui il ricorso regolarizzato perviene all'Ufficio.
2. Il Garante determina i casi in cui è possibile la regolarizzazione del ricorso.

#### **Art. 149. Procedimento relativo al ricorso**

1. Fuori dei casi in cui è dichiarato inammissibile o manifestamente infondato, il ricorso è comunicato al titolare entro tre giorni a cura dell'Ufficio del Garante, con invito ad esercitare entro dieci giorni dal suo ricevimento la facoltà di comunicare al ricorrente e all'Ufficio la propria eventuale adesione spontanea. L'invito è comunicato al titolare per il tramite del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, ove indicato nel ricorso.
2. In caso di adesione spontanea è dichiarato non luogo a provvedere. Se il ricorrente lo richiede, è determinato in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico della controparte o compensati per giusti motivi anche parzialmente.

3. Nel procedimento dinanzi al Garante il titolare, il responsabile di cui al comma 1 e l'interessato hanno diritto di essere sentiti, personalmente o a mezzo di procuratore speciale, e hanno facoltà di presentare memorie o documenti. A tal fine l'invito di cui al comma 1 è trasmesso anche al ricorrente e reca l'indicazione del termine entro il quale il titolare, il medesimo responsabile e l'interessato possono presentare memorie e documenti, nonché della data in cui tali soggetti possono essere sentiti in contraddittorio anche mediante idonea tecnica audiovisiva.
4. Nel procedimento il ricorrente può precisare la domanda nei limiti di quanto chiesto con il ricorso o a seguito di eccezioni formulate dal titolare.
5. Il Garante può disporre, anche d'ufficio, l'espletamento di una o più perizie. Il provvedimento che le dispone precisa il contenuto dell'incarico e il termine per la sua esecuzione, ed è comunicato alle parti le quali possono presenziare alle operazioni personalmente o tramite procuratori o consulenti designati. Il provvedimento dispone inoltre in ordine all'anticipazione delle spese della perizia.
6. Nel procedimento, il titolare e il responsabile di cui al comma 1 possono essere assistiti da un procuratore o da altra persona di fiducia.
7. Se gli accertamenti risultano particolarmente complessi o vi è l'assenso delle parti il termine di sessanta giorni di cui all'articolo 150, comma 2, può essere prorogato per un periodo non superiore ad ulteriori quaranta giorni.
8. Il decorso dei termini previsti dall'articolo 150, comma 2 e dall'articolo 151 è sospeso di diritto dal 1 agosto al 15 settembre di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Se il decorso ha inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussiste il pregiudizio di cui all'articolo 146, comma 1, e non preclude l'adozione dei provvedimenti di cui all'articolo 150, comma 1 .

#### **Art. 150. Provvedimenti a seguito del ricorso**

1. Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento può essere adottato anche prima della comunicazione del ricorso ai sensi dell'articolo 149, comma 1, e cessa di avere ogni effetto se non è adottata nei termini la decisione di cui al comma 2. Il medesimo provvedimento è impugnabile unitamente a tale decisione.
2. Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto.
3. Se vi è stata previa richiesta di taluna delle parti, il provvedimento che definisce il procedimento determina in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico, anche in parte, del soccombente o compensati anche parzialmente per giusti motivi.
4. Il provvedimento espresso, anche provvisorio, adottato dal Garante è comunicato alle parti entro dieci giorni presso il domicilio eletto o risultante dagli atti. Il provvedimento può essere comunicato alle parti anche mediante posta elettronica o telefax.
5. Se sorgono difficoltà o contestazioni riguardo all'esecuzione del provvedimento di

cui ai commi 1 e 2, il Garante, sentite le parti ove richiesto, dispone le modalità di attuazione avvalendosi, se necessario, del personale dell'Ufficio o della collaborazione di altri organi dello Stato.

6. In caso di mancata opposizione avverso il provvedimento che determina l'ammontare delle spese e dei diritti, o di suo rigetto, il provvedimento medesimo costituisce, per questa parte, titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

#### **Art. 151. Opposizione**

1. Avverso il provvedimento espresso o il rigetto tacito di cui all'articolo 150, comma 2, il titolare o l'interessato possono proporre opposizione con ricorso ai sensi dell'articolo 152. L'opposizione non sospende l'esecuzione del provvedimento.

2. Il tribunale provvede nei modi di cui all'articolo 152.

## **CAPO II - TUTELA GIURISDIZIONALE**

#### **Art. 152. Autorità giudiziaria ordinaria**

1. Tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.

2. Per tutte le controversie di cui al comma 1 l'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento.

3. Il tribunale decide in ogni caso in composizione monocratica.

4. Se è presentato avverso un provvedimento del Garante anche ai sensi dell'articolo 143, il ricorso è proposto entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito.

Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione.

5. La proposizione del ricorso non sospende l'esecuzione del provvedimento del Garante. Se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio.

6. Quando sussiste pericolo imminente di un danno grave ed irreparabile il giudice può emanare i provvedimenti necessari con decreto motivato, fissando, con il medesimo provvedimento, l'udienza di comparizione delle parti entro un termine non superiore a quindici giorni. In tale udienza, con ordinanza, il giudice conferma, modifica o revoca i provvedimenti emanati con decreto.

7. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.

8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.

9. Nel corso del giudizio il giudice dispone, anche d'ufficio, omettendo ogni formalità non necessaria al contraddittorio, i mezzi di prova che ritiene necessari e può disporre la citazione di testimoni anche senza la formulazione di capitoli.

10. Terminata l'istruttoria, il giudice invita le parti a precisare le conclusioni ed a procedere, nella stessa udienza, alla discussione orale della causa, pronunciando subito dopo la sentenza mediante lettura del dispositivo. Le motivazioni della sentenza sono depositate in cancelleria entro i successivi trenta giorni. Il giudice può anche redigere e leggere, unitamente al dispositivo, la motivazione della sentenza, che è subito dopo depositata in cancelleria.

11. Se necessario, il giudice può concedere alle parti un termine non superiore a dieci giorni per il deposito di note difensive e rinviare la causa all'udienza immediatamente successiva alla scadenza del termine per la discussione e la pronuncia della sentenza.

12. Con la sentenza il giudice, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), quando è necessario anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento.

13. La sentenza non è appellabile, ma è ammesso il ricorso per cassazione.

14. Le disposizioni di cui al presente articolo si applicano anche nei casi previsti dall'articolo 10, comma 5, della legge 1 aprile 1981, n. 121, e successive modificazioni.

## **TITOLO II - L'AUTORITÀ**

### **CAPO I - IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

#### **Art. 153. Il Garante**

1. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.

2. Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

3. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

4. Il presidente e i componenti durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, nè essere amministratori o dipendenti di enti pubblici o privati, nè ricoprire cariche elettive.

5. All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n.

382, e successive modificazioni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.

6. Al presidente compete una indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai componenti compete un'indennità non eccedente nel massimo, i due terzi di quella spettante al presidente. Le predette indennità di funzione sono determinate dall'articolo 6 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501, in misura tale da poter essere corrisposte a carico degli ordinari stanziamenti.

7. Alle dipendenze del Garante è posto l'Ufficio di cui all'articolo 156.

#### **Art. 154. Compiti**

1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di:

- a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione;
  - b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;
  - c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;
  - d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporre il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;
  - e) promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'articolo 139;
  - f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti di cui all'articolo 2 anche a seguito dell'evoluzione del settore;
  - g) esprimere pareri nei casi previsti;
  - h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati;
  - i) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;
  - l) tenere il registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37;
  - m) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.
2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari e, in particolare:
- a) dalla legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'accordo di Schengen e alla relativa convenzione di applicazione;
  - b) dalla legge 23 marzo 1998, n. 93, e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (Europol);
  - c) dal regolamento (Ce) n. 515/97 del Consiglio, del 13 marzo 1997, e dalla legge 30

- luglio 1998, n. 291, e successive modificazioni, di ratifica ed esecuzione della convenzione sull'uso dell'informatica nel settore doganale;
- d) dal regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino;
- e) nel capitolo IV della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.
3. Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità.
4. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dal presente codice.
5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante è reso nei casi previsti nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.
6. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalità informatica è trasmessa, a cura della cancelleria, al Garante.

## **CAPO II - L'UFFICIO DEL GARANTE**

### **Art. 155. Principi applicabili**

1. All'Ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge 7 agosto 1990, n. 241, e successive modificazioni, e del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e le funzioni di gestione attribuite ai dirigenti. Si applicano altresì le disposizioni del medesimo decreto legislativo n. 165 del 2001 espressamente richiamate.

#### **Art. 156. Ruolo organico e personale**

1. All'Ufficio del Garante è preposto un segretario generale scelto anche tra magistrati ordinari o amministrativi.
2. Il ruolo organico del personale dipendente è stabilito nel limite di cento unità.
3. Con propri regolamenti pubblicati nella Gazzetta ufficiale della Repubblica italiana, il Garante definisce:
  - a) l'organizzazione e il funzionamento dell'ufficio anche ai fini dello svolgimento dei compiti di cui all'articolo 154;
  - b) l'ordinamento delle carriere e le modalità di reclutamento del personale secondo le procedure previste dall'articolo 35 del decreto legislativo n. 165 del 2001;
  - c) la ripartizione dell'organico tra le diverse aree e qualifiche;
  - d) il trattamento giuridico ed economico del personale, secondo i criteri previsti dalla legge 31 luglio 1997, n. 249, e successive modificazioni e, per gli incarichi dirigenziali, dagli articoli 19, comma 6, e 23 *bis* del decreto legislativo 30 marzo 2001, n. 165, tenuto conto delle specifiche esigenze funzionali e organizzative. Nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti, al personale è attribuito l'ottanta per cento del trattamento economico del personale dell'Autorità per le garanzie nelle comunicazioni;
  - e) la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato, l'utilizzo dell'avanzo di amministrazione nel quale sono iscritte le somme già versate nella contabilità speciale, nonché l'individuazione dei casi di riscossione e utilizzazione dei diritti di segreteria o di corrispettivi per servizi resi in base a disposizioni di legge secondo le modalità di cui all'articolo 6, comma 2, della legge 31 luglio 1997, n. 249.
4. L'Ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni, in numero non superiore, complessivamente, a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo. Al personale di cui al presente comma è corrisposta un'indennità pari all'eventuale differenza tra il trattamento erogato dall'amministrazione o dall'ente di provenienza e quello spettante al personale di ruolo, sulla base di apposita tabella di corrispondenza adottata dal Garante, e comunque non inferiore al cinquanta per cento della retribuzione in godimento, con esclusione dell'indennità integrativa speciale.
5. In aggiunta al personale di ruolo, l'ufficio può assumere direttamente dipendenti con contratto a tempo determinato, in numero non superiore a venti unità ivi compresi i consulenti assunti con contratto a tempo determinato ai sensi del comma 7.
6. Si applicano le disposizioni di cui all'articolo 30 del decreto legislativo n. 165 del 2001.
7. Nei casi in cui la natura tecnica o la delicatezza dei problemi lo richiedono, il Garante può avvalersi dell'opera di consulenti, i quali sono remunerati in base alle vigenti tariffe professionali ovvero sono assunti con contratti a tempo determinato, di durata non superiore a due anni, che possono essere rinnovati per non più di due

volte.

8. Il personale addetto all'Ufficio del Garante ed i consulenti sono tenuti al segreto su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

9. Il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'articolo 158 riveste, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.

10. Le spese di funzionamento del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti.

### **CAPO III - ACCERTAMENTI E CONTROLLI**

#### **Art. 157. Richiesta di informazioni e di esibizione di documenti**

1. Per l'espletamento dei propri compiti il Garante può richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti.

#### **Art. 158. Accertamenti**

1. Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1 sono eseguiti da personale dell'Ufficio. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato.

3. Gli accertamenti di cui al comma 1, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

#### **Art. 159. Modalità**

1. Il personale operante, munito di documento di riconoscimento, può essere assistito ove necessario da consulenti tenuti al segreto ai sensi dell'articolo 156, comma 8. Nel procedere a rilievi e ad operazioni tecniche può altresì estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Degli accertamenti è redatto sommario verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

2. Ai soggetti presso i quali sono eseguiti gli accertamenti è consegnata copia dell'autorizzazione del presidente del tribunale, ove rilasciata. I medesimi soggetti sono tenuti a farli eseguire e a prestare la collaborazione a tal fine necessaria. In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese in tal caso occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento,

che per questa parte costituisce titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

3. Gli accertamenti, se effettuati presso il titolare o il responsabile, sono eseguiti dandone informazione a quest'ultimo o, se questo è assente o non è designato, agli incaricati. Agli accertamenti possono assistere persone indicate dal titolare o dal responsabile.

4. Se non è disposto diversamente nel decreto di autorizzazione del presidente del tribunale, l'accertamento non può essere iniziato prima delle ore sette e dopo le ore venti, e può essere eseguito anche con preavviso quando ciò può facilitarne l'esecuzione.

5. Le informative, le richieste e i provvedimenti di cui al presente articolo e agli articoli 157 e 158 possono essere trasmessi anche mediante posta elettronica e telefax.

6. Quando emergono indizi di reato si osserva la disposizione di cui all'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271.

#### **Art. 160. Particolari accertamenti**

1. Per i trattamenti di dati personali indicati nei titoli I, II e III della Parte II gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.

2. Se il trattamento non risulta conforme alle disposizioni di legge o di regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, se ciò non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato.

3. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere da personale specializzato tenuto al segreto ai sensi dell'articolo 156, comma 8. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal regolamento di cui all'articolo 156, comma 3, lettera a).

4. Per gli accertamenti relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

5. Nell'effettuare gli accertamenti di cui al presente articolo nei riguardi di uffici giudiziari, il Garante adotta idonee modalità nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo precedente. Gli accertamenti riferiti ad atti di indagine coperti dal segreto sono differiti, se vi è richiesta dell'organo precedente, al momento in cui cessa il segreto.

6. La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale.

## **TITOLO III - SANZIONI**

### **CAPO I - VIOLAZIONI AMMINISTRATIVE**

#### **Art. 161. Omessa o inidonea informativa all'interessato**

1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

#### **Art. 162. Altre fattispecie**

1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro.

2. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da cinquecento euro a tremila euro.

#### **Art. 163. Omessa o incompleta notificazione**

1. 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 diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

#### **Art. 164. Omessa informazione o esibizione al Garante**

1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma da quattromila euro a ventiquattro mila euro.

#### **Art. 165. Pubblicazione del provvedimento del Garante**

1. Nei casi di cui agli articoli 161, 162 e 164 può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

#### **Art. 166. Procedimento di applicazione**

1. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente capo e all'articolo 179, comma 3, è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive

modificazioni. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 10, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 154, comma 1, lettera h), e 158.

## **CAPO II - ILLECITI PENALI**

### **Art. 167. Trattamento illecito di dati**

1. 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, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. 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, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

### **Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante**

1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

### **Art. 169. Misure di sicurezza**

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

### **Art. 170. Inosservanza di provvedimenti del Garante**

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

**Art. 171. Altre fattispecie**

1. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

**Art. 172. Pene accessorie**

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

**TITOLO IV - DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI**

**CAPO II - DISPOSIZIONI TRANSITORIE**

**Art. 180. Misure di sicurezza**

1. Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 30 giugno 2004.

2. Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura.

3. Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro un anno dall'entrata in vigore del codice.

**Art. 181. Altre disposizioni transitorie**

1. Per i trattamenti di dati personali iniziati prima del 1 gennaio 2004, in sede di prima applicazione del presente codice:

a) l'identificazione con atto di natura regolamentare dei tipi di dati e di operazioni ai sensi degli articoli 20, commi 2 e 3, e 21, comma 2, è effettuata, ove mancante, entro il 30 settembre 2004;

b) la determinazione da rendere nota agli interessati ai sensi dell'articolo 26, commi 3, lettera a), e 4, lettera a), è adottata, ove mancante, entro il 30 giugno 2004;

c) le notificazioni previste dall'articolo 37 sono effettuate entro il 30 aprile 2004;

d) le comunicazioni previste dall'articolo 39 sono effettuate entro il 30 giugno 2004;

e) le modalità semplificate per l'informativa e la manifestazione del consenso, ove necessario, possono essere utilizzate dal medico di medicina generale, dal pediatra di libera scelta e dagli organismi sanitari anche in occasione del primo ulteriore contatto con l'interessato, al più tardi entro il 30 settembre 2004;

f) l'utilizzazione dei modelli di cui all'articolo 87, comma 2, è obbligatoria a decorrere dal 1 gennaio 2005.

2. Le disposizioni di cui all'articolo 21 *bis* del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, introdotto dall'articolo 9 del decreto legislativo 30 luglio

1999, n. 281, restano in vigore fino alla data di entrata in vigore del presente codice.

3. L'individuazione dei trattamenti e dei titolari di cui agli articoli 46 e 53, da riportare nell'allegato C), è effettuata in sede di prima applicazione del presente codice entro il 30 giugno 2004.

4. Il materiale informativo eventualmente trasferito al Garante ai sensi dell'articolo 43, comma 1, della legge 31 dicembre 1996, n. 675, utilizzato per le opportune verifiche, continua ad essere successivamente archiviato o distrutto in base alla normativa vigente.

5. L'omissione delle generalità e degli altri dati identificativi dell'interessato ai sensi dell'articolo 52, comma 4, è effettuata sulle sentenze o decisioni pronunciate o adottate prima dell'entrata in vigore del presente codice solo su diretta richiesta dell'interessato e limitatamente ai documenti pubblicati mediante rete di comunicazione elettronica o sui nuovi prodotti su supporto cartaceo o elettronico. I sistemi informativi utilizzati ai sensi dell'articolo 51, comma 1, sono adeguati alla medesima disposizione entro dodici mesi dalla data di entrata in vigore del presente codice.

6. Le confessioni religiose che, prima dell'adozione del presente codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui all'articolo 26, comma 3, lettera a), possono proseguire l'attività di trattamento nel rispetto delle medesime.

6-bis. Fino alla data in cui divengono efficaci le misure e gli accorgimenti prescritti ai sensi dell'articolo 132, comma 5, per la conservazione del traffico telefonico si osserva il termine di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171.

#### **Art. 182. Ufficio del Garante**

1. Al fine di assicurare la continuità delle attività istituzionali, in sede di prima applicazione del presente codice e comunque non oltre il 31 marzo 2004, il Garante:

a) può individuare i presupposti per l'inquadramento in ruolo, al livello iniziale delle rispettive qualifiche e nei limiti delle disponibilità di organico, del personale appartenente ad amministrazioni pubbliche o ad enti pubblici in servizio presso l'Ufficio del Garante in posizione di fuori ruolo o equiparato alla data di pubblicazione del presente codice;

b) può prevedere riserve di posti nei concorsi pubblici, unicamente nel limite del trenta per cento delle disponibilità di organico, per il personale non di ruolo in servizio presso l'Ufficio del Garante che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno.

### **CAPO III - ABROGAZIONI**

#### **Art. 183. Norme abrogate**

1. Dalla data di entrata in vigore del presente codice sono abrogati:

a) la legge 31 dicembre 1996, n. 675;

b) la legge 3 novembre 2000, n. 325;

c) il decreto legislativo 9 maggio 1997, n. 123;

d) il decreto legislativo 28 luglio 1997, n. 255;

e) l'articolo 1 del decreto legislativo 8 maggio 1998, n. 135;

- f) il decreto legislativo 13 maggio 1998, n. 171;
  - g) il decreto legislativo 6 novembre 1998, n. 389;
  - h) il decreto legislativo 26 febbraio 1999, n. 51;
  - i) il decreto legislativo 11 maggio 1999, n. 135;
  - l) il decreto legislativo 30 luglio 1999, n. 281, ad eccezione degli articoli 8, comma 1, 11 e 12;
  - m) il decreto legislativo 30 luglio 1999, n. 282;
  - n) il decreto legislativo 28 dicembre 2001, n. 467;
  - o) il decreto del Presidente della Repubblica 28 luglio 1999, n. 318.
2. Dalla data di entrata in vigore del presente codice sono abrogati gli articoli 12, 13, 14, 15, 16, 17, 18, 19 e 20 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501.
3. Dalla data di entrata in vigore del presente codice sono o restano, altresì, abrogati:
- a) l'art. 5, comma 9, del decreto del Ministro della sanità 18 maggio 2001, n. 279, in materia di malattie rare;
  - b) l'articolo 12 della legge 30 marzo 2001, n. 152;
  - c) l'articolo 4, comma 3, della legge 6 marzo 2001, n. 52, in materia di donatori midollo osseo;
  - d) l'articolo 16, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, in materia di certificati di assistenza al parto;
  - e) l'art. 2, comma 5, del decreto del Ministro della sanità 27 ottobre 2000, n. 380, in materia di flussi informativi sui dimessi dagli istituti di ricovero;
  - f) l'articolo 2, comma 5 *quater* 1, secondo e terzo periodo, del decreto legge 28 marzo 2000, n. 70, convertito, con modificazioni, dalla legge 26 maggio 2000, n. 137, e successive modificazioni, in materia di banca dati sinistri in ambito assicurativo;
  - g) l'articolo 6, comma 4, del decreto legislativo 5 giugno 1998, n. 204, in materia di diffusione di dati a fini di ricerca e collaborazione in campo scientifico e tecnologico;
  - h) l'articolo 330 *bis* del decreto legislativo 16 aprile 1994, n. 297, in materia di diffusione di dati relativi a studenti;
  - i) l'articolo 8, quarto comma, e l'articolo 9, quarto comma, della legge 1 aprile 1981, n. 121.
4. Dalla data in cui divengono efficaci le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 118, i termini di conservazione dei dati personali individuati ai sensi dell'articolo 119, eventualmente previsti da norme di legge o di regolamento, si osservano nella misura indicata dal medesimo codice.

#### **CAPO IV - NORME FINALI**

##### **Art. 184. Attuazione di direttive europee**

1. Le disposizioni del presente codice danno attuazione alla direttiva 96/45/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, e alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002.
2. Quando leggi, regolamenti e altre disposizioni fanno riferimento a disposizioni comprese nella legge 31 dicembre 1996, n. 675, e in altre disposizioni abrogate dal presente codice, il riferimento si intende effettuato alle corrispondenti disposizioni del presente codice secondo la tavola di corrispondenza riportata in allegato.

3. Restano ferme le disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

**Art. 185. Allegazione dei codici di deontologia e di buona condotta**

1. L'allegato A) riporta, oltre ai codici di cui all'articolo 12, commi 1 e 4, quelli promossi ai sensi degli articoli 25 e 31 della legge 31 dicembre 1996, n. 675, e già pubblicati nella Gazzetta Ufficiale della Repubblica italiana alla data di emanazione del presente codice.

**Art. 186. Entrata in vigore**

1. Le disposizioni di cui al presente codice entrano in vigore il 1 gennaio 2004, ad eccezione delle disposizioni di cui agli articoli 156, 176, commi 3, 4, 5 e 6, e 182, che entrano in vigore il giorno successivo alla data di pubblicazione del presente codice. Dalla medesima data si osservano altresì i termini in materia di ricorsi di cui agli articoli 149, comma 8, e 150, comma 2.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

*Dato a Roma, addì 30 giugno 2003*

**ALLEGATO B - DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA**

(Artt. da 33 a 36 del Codice)

**Trattamenti con strumenti elettronici**

**Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:**

**Sistema di autenticazione informatica**

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da

almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

#### **Sistema di autorizzazione**

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

#### **Altre misure di sicurezza**

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è

almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

**Documento programmatico sulla sicurezza**

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

**Ulteriori misure in caso di trattamento di dati sensibili o giudiziari**

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati

relativi

all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

**Misure di tutela e garanzia**

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

**Trattamenti senza l'ausilio di strumenti elettronici**

**Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:**

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. 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 dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

## **la deliberazione 31 marzo 2004, n. 1 - “Casi da sottrarre all'obbligo di notificazione al Garante”**

Il Garante per la protezione dei dati personali

In data odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 37, commi 1 e 2, del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Rilevato che tale Codice indica i trattamenti di dati da notificare al Garante e demanda a questa Autorità il compito di individuare, tra essi, quelli sottratti all'obbligo di notificazione purché non suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle modalità di trattamento o della natura dei dati (art. 37, comma 1);

Rilevato che il medesimo Codice demanda altresì al Garante il compito di individuare ulteriori trattamenti in aggiunta a quelli elencati nella predetta disposizione;

Vista la documentazione in atti;

Rilevato in sede di prima applicazione del Codice che taluni trattamenti sono effettuati con modalità che permettono, allo stato, di sottrarli all'obbligo di notificazione, ferma restando l'osservanza degli ulteriori principi ed obblighi previsti dal Codice in materia di protezione dei dati personali;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Stefano Rodotà;

Delibera:

di sottrarre all'obbligo di notificazione al Garante, tra i casi previsti dall'art. 37, comma 1, del decreto legislativo 30 giugno 2003, n. 196:

1) con riferimento ai casi di cui al comma 1, lettera a) di tale disposizione:

i trattamenti non sistematici di dati genetici o biometrici effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica. Ciò limitatamente ai dati e alle operazioni, compresa la comunicazione, indispensabili per perseguire finalità di tutela della salute o dell'incolumità fisica dell'interessato o di un terzo;

i trattamenti di dati genetici o biometrici effettuati nell'esercizio della professione di avvocato, in relazione alle operazioni e ai dati necessari per svolgere le investigazioni difensive di cui alla legge n. 397/2000, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria. Ciò sempre che il diritto sia di rango almeno pari a quello dell'interessato e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

i trattamenti di dati che indicano la posizione geografica di mezzi di trasporto aereo,

navale e terrestre, effettuati esclusivamente a fini di sicurezza del trasporto;

2) con riferimento ai casi di cui al comma 1, lettera b) della medesima disposizione, i trattamenti di dati idonei a rivelare lo stato di salute e la vita sessuale effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti:

a fini di procreazione assistita, di trapianto di organi e tessuti, indagine epidemiologica, rilevazione di malattie mentali, infettive, diffuse o di sieropositività. Ciò sempre che i trattamenti siano effettuati non sistematicamente, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica e limitatamente ai dati e alle operazioni indispensabili per la tutela della salute o dell'incolumità fisica dell'interessato o di un terzo;

ad esclusivi fini di monitoraggio della spesa sanitaria o di adempimento di obblighi normativi in materia di igiene e sicurezza del lavoro e della popolazione;

3) con riferimento ai casi di cui al comma 1, lettera c), i trattamenti di dati idonei a rivelare la sfera psichica di lavoratori:

effettuati da associazioni, enti od organismi a carattere sindacale per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di rapporto di lavoro o di previdenza, anche in tema di diritto al lavoro dei disabili;

effettuati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico o religioso riguardo a dati di propri dipendenti o collaboratori, per adempiere esclusivamente a specifici obblighi previsti dalla normativa in materia di rapporto di lavoro o di previdenza;

4) con riferimento ai casi di cui al comma 1, lettera d), i trattamenti di dati personali: che non siano fondati unicamente su un trattamento automatizzato volto a definire profili professionali, effettuati per esclusive finalità di occupazione o di gestione del rapporto di lavoro, fuori dei casi di cui alla lettera e) del medesimo art. 37, comma 1;

che non siano fondati unicamente su un trattamento automatizzato volto a definire il profilo di un investitore, effettuati esclusivamente per adempiere a specifici obblighi previsti dalla normativa in materia di intermediazione finanziaria;

relativi all'utilizzo di marcatori elettronici o di dispositivi analoghi installati, oppure memorizzati temporaneamente, e non persistenti, presso l'apparecchiatura terminale di un utente, consistenti nella sola trasmissione di identificativi di sessione in conformità alla disciplina applicabile, all'esclusivo fine di agevolare l'accesso ai contenuti di un sito Internet;

5) con riferimento ai casi di cui al comma 1, lettera e), i trattamenti di dati sensibili effettuati:

al solo fine di selezione di personale per conto esclusivamente di soggetti appartenenti al medesimo gruppo bancario o societario;

da soggetti pubblici per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di occupazione e mercato del lavoro;

da associazioni o organizzazioni di categoria al solo fine di svolgere ricerche campionarie relativamente a dati riguardanti l'adesione alla medesima associazione o organizzazione;

6) con riferimento ai casi di cui al comma 1, lettera f), i trattamenti di dati personali: effettuati da soggetti pubblici per la tenuta di pubblici registri o elenchi conoscibili da chiunque;  
registrati in banche di dati utilizzate in rapporti con l'interessato di fornitura di beni, prestazioni o servizi, o per adempimenti contabili o fiscali, anche in caso di inadempimenti contrattuali, azioni di recupero del credito e contenzioso con l'interessato;  
registrati in banche di dati utilizzate da soggetti pubblici o privati per adempiere esclusivamente ad obblighi normativi in materia di rapporto di lavoro, previdenza o assistenza;  
registrati in banche di dati utilizzate da soggetti pubblici al solo fine della tenuta ed esecuzione di atti, provvedimenti e documenti, in tema di riscossione di tributi, applicazione di sanzioni amministrative, o rilascio di licenze, concessioni o autorizzazioni;  
relativi a immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio;  
trattati, in base alla legge, dai soggetti autorizzati in relazione alle operazioni e ai dati necessari all'esclusivo fine di prestare l'attività di garanzia collettiva dei fidi e i servizi a essa connessi o strumentali ("confidi");

B) di inviare copia della presente deliberazione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia ai fini della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.”

## **autorizzazione n. 1/2004 al trattamento dei dati sensibili nei rapporti di lavoro**

### **Il Garante per la protezione dei dati personali**

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. d), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto il comma 4, lett. d), del medesimo art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento medesimo 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, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'art. 111 del Codice;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione del codice di deontologia e buona condotta di cui all'art. 111 del Codice;

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e, in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato

nell'ambito dei rapporti di lavoro;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B al medesimo Codice recanti norme e regole sulle misure di sicurezza;

Visto l'art. 41 del Codice;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il prof. Stefano Rodotà;

#### **Autorizza**

il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. d), del Codice, finalizzato alla gestione dei rapporti di lavoro, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

#### **1) Ambito di applicazione**

La presente autorizzazione è rilasciata:

- a) alle persone fisiche e giuridiche, alle imprese, agli enti, alle associazioni e agli organismi che sono parte di un rapporto di lavoro o che utilizzano prestazioni lavorative anche atipiche, parziali o temporanee, o che comunque conferiscono un incarico professionale alle figure indicate al successivo punto 2, lett. b) e c);
- b) ad organismi paritetici o che gestiscono osservatori in materia di lavoro, previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi anche aziendali;

L'autorizzazione riguarda anche l'attività svolta:

- c) dal medico competente in materia di igiene e di sicurezza del lavoro, in qualità di libero professionista o di dipendente dei soggetti di cui alla lettera a) o di strutture convenzionate;
- d) da associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro, al solo fine di perseguire le finalità di cui al punto 3), lett. h).

#### **2) Interessati ai quali i dati si riferiscono**

Il trattamento può riguardare i dati sensibili attinenti:

- a) 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 in base ai punti 3) e 4), ai relativi familiari e conviventi;

- b) a consulenti e a liberi professionisti, ad agenti, rappresentanti e mandatari;
- c) a soggetti che effettuano prestazioni coordinate e continuative o ad altri lavoratori autonomi in rapporto di collaborazione con i soggetti di cui al punto 1);
- d) a candidati all'instaurazione dei rapporti di lavoro di cui alle lettere precedenti;
- e) a persone fisiche che ricoprono cariche sociali o altri incarichi nelle persone giuridiche, negli enti, nelle associazioni e negli organismi di cui al punto 1);
- f) a terzi danneggiati nell'esercizio dell'attività lavorativa o professionale dai soggetti di cui alle precedenti lettere.

### **3) Finalità del trattamento**

Il trattamento dei dati sensibili deve essere indispensabile:

- a) 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;
- b) anche fuori dei casi di cui alla lettera a), 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;
- c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo;
- d) 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;
- e) per esercitare il diritto di accesso ai documenti amministrativi, nel rispetto di quanto stabilito dalle leggi e dai regolamenti in materia;
- f) 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;
- g) per garantire le pari opportunità;
- h) 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.

### **4) Categorie di dati**

Il trattamento può avere per oggetto i dati strettamente pertinenti ai sopra indicati obblighi, compiti o finalità che non possano essere adempiuti o realizzati, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, e in particolare:

- a) nell'ambito dei dati idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico, i dati concernenti la fruizione di permessi e festività religiose o di servizi di mensa, nonché la manifestazione, nei casi previsti dalla legge, dell'obiezione di coscienza;
- b) nell'ambito dei dati idonei a rivelare le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere politico o sindacale, i dati 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 i dati inerenti alle trattenute per il versamento delle quote di servizio sindacale o delle quote di iscrizione ad associazioni od organizzazioni politiche o sindacali;
- c) nell'ambito dei dati idonei a rivelare lo stato di salute, i dati 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 i 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.

#### **5) Modalità di trattamento**

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, nonché dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

I dati sono raccolti, di regola, presso l'interessato.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia. Restano inoltre 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.

#### **6) Conservazione dei dati**

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e), del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per adempiere agli obblighi o ai compiti di cui al punto 3), ovvero per perseguire le finalità ivi menzionate. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale

conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

#### **7) Comunicazione e diffusione dei dati**

I dati sensibili possono essere comunicati e, ove necessario diffusi, nei limiti strettamente pertinenti agli obblighi, ai compiti o alle finalità di cui al punto 3), a soggetti pubblici o privati, ivi compresi organismi sanitari, casse e fondi di previdenza ed assistenza sanitaria integrativa anche aziendale, istituti di patronato e di assistenza sociale, centri di assistenza fiscale, agenzie per il lavoro, associazioni ed organizzazioni sindacali di datori di lavoro e di prestatori di lavoro, liberi professionisti, società esterne titolari di un autonomo trattamento di dati e familiari dell'interessato.

Ai sensi dell'art. 26, comma 5, del Codice, i dati idonei a rivelare lo stato di salute non possono essere diffusi.

#### **8) Richieste di autorizzazione**

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità dalle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

#### **9) Norme finali.**

Restano fermi gli obblighi previsti da norme di legge o di regolamento, ovvero dalla normativa comunitaria, che stabiliscono divieti o limiti in materia di trattamento di dati personali e, in particolare, dalle disposizioni contenute:

- a) nell'art. 8 della legge 20 maggio 1970, n. 300, che vieta al datore di lavoro ai fini dell'assunzione e nello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;
- b) nell'art. 6 della legge 5 giugno 1990, n. 135, che vieta ai datori di lavoro lo svolgimento di indagini volte ad accertare, nei dipendenti o in persone prese in considerazione per l'instaurazione di un rapporto di lavoro, l'esistenza di uno stato di sieropositività;
- c) nelle norme in materia di pari opportunità o volte a prevenire discriminazioni;
- d) fermo restando quanto disposto dall'art. 8 della legge 20 maggio 1970, n. 300, nell'art. 10 del d.lg. 10 settembre 2003, n. 276, che vieta alle agenzie per il lavoro e agli altri soggetti privati autorizzati o accreditati di effettuare qualsivoglia indagine o

comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute e ad eventuali controversie con i precedenti datori di lavoro, nonché di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo.

**10) Efficacia temporale e disciplina transitoria.**

La presente autorizzazione ha efficacia a decorrere dal 1 luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 1/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.<sup>10</sup>

Roma, 30 giugno 2004

---

<sup>10</sup> G.U. n. 190 del 14 agosto 2004

## **autorizzazione n. 5/2004 al trattamento dei dati sensibili da parte di diverse categorie di titolari**

### **Il Garante per la protezione dei dati personali**

In data odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vicepresidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. d) del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;

Ritenuto opportuno, dopo l'entrata in vigore del Codice, rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2004, armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata tenuto conto dei codici di deontologia e di buona condotta di cui agli articoli 106 e 140 del Codice;

Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato ai sensi dell'art. 41, comma 5, del Codice, e, in particolare, efficaci per il periodo di dodici mesi, in relazione alla fase di prima applicazione delle nuove disposizioni del Codice e ai lavori avviati per l'adozione dei codici di deontologia e di buona condotta riguardanti alcuni specifici settori presi in considerazione dal presente provvedimento (articoli 111 e 140 del Codice);

Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e in particolare, per il diritto alla protezione dei dati personali sancito all'art. 1 del Codice;

Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da parte di soggetti operanti in diversi settori di attività economiche di seguito individuate;

Visto l'art. 167 del Codice;

Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;

Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B al medesimo Codice recanti norme e regole sulle misure di sicurezza;  
Visto l'art. 41 del Codice;  
Visti gli atti d'ufficio;  
Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;  
Relatore il prof. Gaetano Rasi;

#### **Autorizza**

il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. d), del Codice, fatta eccezione dei dati idonei a rivelare la vita sessuale, secondo le prescrizioni di seguito indicate.

Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

#### **Capo I - Attività bancarie, creditizie, assicurative, di gestione di fondi, del settore turistico, del trasporto**

##### **1) Soggetti ai quali è rilasciata l'autorizzazione:**

- a) imprese autorizzate all'esercizio dell'attività bancaria e creditizia o assicurativa ed organismi che le riuniscono, anche se in stato di liquidazione coatta amministrativa;
- b) società ed altri organismi che gestiscono fondi-pensione o di assistenza, ovvero fondi o casse di previdenza;
- c) società ed altri organismi di intermediazione finanziaria, in particolare per la gestione o l'intermediazione di fondi comuni di investimento o di valori mobiliari;
- d) società ed altri organismi che emettono carte di credito o altri mezzi di pagamento, o che ne gestiscono le relative operazioni;
- e) imprese che svolgono autonome attività strettamente connesse e strumentali a quelle indicate nelle precedenti lettere, e relative alla rilevazione dei rischi, al recupero dei crediti, a lavorazioni massive di documenti, alla trasmissione dati, all'imbustamento o allo smistamento della corrispondenza, nonché alla gestione di esattorie o tesorerie;
- f) imprese che operano nel settore turistico o alberghiero o del trasporto, agenzie di viaggio e operatori turistici.

##### **2) Finalità del trattamento**

La presente autorizzazione è rilasciata, anche senza richiesta, limitatamente ai dati e alle operazioni indispensabili per adempiere agli obblighi anche precontrattuali che i soggetti di cui al punto 1) assumono, nel proprio settore di attività, al fine di fornire specifici beni, prestazioni o servizi richiesti dall'interessato.

L'autorizzazione è rilasciata anche per adempiere o per esigere l'adempimento ad obblighi previsti, anche in materia fiscale e contabile, dalla normativa comunitaria, dalla legge, dai regolamenti, o dai contratti collettivi, o prescritti da autorità od organi

di vigilanza o di controllo nei casi indicati dalla legge o dai regolamenti.  
Il trattamento avente tali finalità può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per espletare compiti di organizzazione o di gestione amministrativa di imprese, società, cooperative o consorzi.

### **3) Interessati ai quali i dati si riferiscono e categorie di dati trattati**

Il trattamento può riguardare i dati sensibili attinenti ai soggetti ai quali sono forniti i beni, le prestazioni o i servizi, in misura strettamente pertinente a quanto specificamente richiesto dall'interessato che, ove necessario, abbia manifestato il proprio consenso scritto ed informato. Nei medesimi limiti, è possibile trattare dati relativi a terzi, allorché non sia altrimenti possibile procedere alla fornitura al beneficiario dei beni, delle prestazioni o dei servizi.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

### **4) Comunicazione e diffusione dei dati**

I dati sensibili possono essere comunicati, nei limiti strettamente pertinenti al perseguimento delle finalità di cui al punto 2), a soggetti pubblici o privati, ivi compresi fondi e casse di previdenza ed assistenza o società controllate e collegate ai sensi dell'art. 2359 del codice civile, nonché, ove necessario, ai familiari dell'interessato.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 7, comma 3, lett. c), del Codice), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

I dati sensibili non possono essere diffusi.

## **Capo II - Sondaggi e ricerche**

### **1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento.**

Imprese, società, istituti ed altri organismi o soggetti privati, ai soli fini del compimento di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il sondaggio o la ricerca devono essere effettuati per scopi puntualmente determinati e legittimi, noti all'interessato.

### **2) Interessati ai quali i dati si riferiscono e categorie di dati trattati.**

Il trattamento può riguardare i dati attinenti ai soggetti che abbiano manifestato il proprio consenso informato e che abbiano risposto a questionari o ad interviste effettuate nell'ambito di sondaggi di opinione, di ricerche di mercato o di altre ricerche campionarie.

Il consenso deve essere manifestato in ogni caso per iscritto.

I dati personali di natura sensibile possono essere trattati solo se il trattamento di dati anonimi non permette al sondaggio o alla ricerca di raggiungere i suoi scopi.

### **3) Conservazione dei dati.**

Il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, neanche indirettamente, mediante un riferimento ad una qualsiasi altra informazione.

I dati personali, individuali o aggregati, devono essere distrutti o resi anonimi subito dopo la raccolta, e comunque non oltre la fase contestuale alla registrazione dei campioni raccolti. La registrazione deve essere effettuata senza ritardo anche nel caso in cui i campioni siano stati raccolti in numero elevato.

Entro tale ambito temporale, resta ferma la possibilità per il titolare della raccolta, nonché per i suoi responsabili o incaricati, di utilizzare i dati personali al fine di verificare presso gli interessati la veridicità o l'esattezza dei campioni.

### **4) Comunicazione dei dati**

I dati sensibili non possono essere né comunicati, né diffusi.

I campioni del sondaggio o della ricerca possono essere comunicati o diffusi in forma individuale o aggregata, sempreché non possano essere associati, anche a seguito di trattamento, ad interessati identificati o identificabili.

## **Capo III - Attività di elaborazione di dati**

### **1) Soggetti ai quali è rilasciata l'autorizzazione**

Imprese, società, istituti ed altri organismi o soggetti privati, titolari autonomi di un'attività svolta nell'interesse di altri soggetti, e che presuppone l'elaborazione di dati ed altre operazioni di trattamento eseguite in materia di lavoro ovvero a fini contabili, retributivi, previdenziali, assistenziali e fiscali.

### **2) Prescrizioni applicabili**

Il trattamento è regolato dalle autorizzazioni:

a) n. 1/2004, rilasciata il 30 giugno 2004, concernente il trattamento dei dati sensibili a cura, in particolare, delle parti di un rapporto di lavoro qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione;

b) n. 4/2004, rilasciata il 30 giugno 2004, riguardante il trattamento dei dati sensibili ad opera dei liberi professionisti e di altri soggetti equiparati, qualora le finalità perseguite siano quelle indicate al punto 3) di tale autorizzazione.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

## **Capo IV - Attività di selezione del personale**

### **1) Soggetti ai quali è rilasciata l'autorizzazione e finalità del trattamento**

La presente autorizzazione è rilasciata, anche senza richiesta, alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati, titolari autonomi di attività svolta anche di propria iniziativa nell'interesse di terzi, ai soli fini della ricerca o della selezione del personale.

## **2) Interessati ai quali i dati si riferiscono e categorie di dati trattati**

Il trattamento può riguardare i dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica dei candidati all'instaurazione di un rapporto di lavoro o di collaborazione, solo se la loro raccolta è giustificata da scopi determinati e legittimi ed è strettamente indispensabile per instaurare tale rapporto.

Il trattamento dei dati idonei a rivelare lo stato di salute dei familiari o dei conviventi dei candidati è consentito con il consenso scritto degli interessati e qualora sia finalizzato al riconoscimento di uno specifico beneficio in favore dei candidati, in particolare ai fini di un'assunzione obbligatoria o del riconoscimento di un titolo derivante da invalidità o infermità, da eventi bellici o da ragioni di servizio.

Qualora il consenso sia richiesto nei confronti di distinti titolari di trattamenti, la manifestazione di volontà deve riferirsi specificamente a ciascuno di essi.

Il trattamento deve riguardare le sole informazioni strettamente pertinenti a tale finalità, sia in caso di risposta a questionari inviati anche per via telematica, sia nel caso in cui i candidati forniscano dati di propria iniziativa, in particolare attraverso l'invio di curricula.

Non è consentito il trattamento dei dati:

- a) idonei a rivelare le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni a carattere religioso, filosofico, politico o sindacale, l'origine razziale ed etnica, e la vita sessuale;
- b) inerenti a fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore;
- c) in violazione delle norme in materia di pari opportunità o volte a prevenire discriminazioni.

## **3) Comunicazione e diffusione dei dati**

I dati idonei a rivelare lo stato di salute e l'origine razziale ed etnica possono essere comunicati nei limiti strettamente pertinenti al perseguimento delle finalità di cui ai punti 1) e 2), a soggetti pubblici o privati che siano specificamente menzionati nella dichiarazione di consenso dell'interessato.

I dati sensibili non possono essere diffusi.

## **4) Norme finali**

Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti.

## **Capo V - Mediazione a fini matrimoniali**

### **1) Soggetti ai quali è rilasciata l'autorizzazione**

La presente autorizzazione è rilasciata alle imprese, alle società, agli istituti e agli altri organismi o soggetti privati che esercitano, anche attraverso agenzie autorizzate, un'attività di mediazione a fini matrimoniali o di instaurazione di un rapporto di convivenza.

### **2) Finalità del trattamento**

L'autorizzazione è rilasciata ai soli fini dell'esecuzione dei singoli incarichi conferiti in conformità alle leggi e ai regolamenti.

### **3) Interessati ai quali i dati si riferiscono.**

Il trattamento può riguardare i soli dati sensibili attinenti alle persone direttamente interessate al matrimonio o alla convivenza.

Non è consentito il trattamento di dati relativo a persone minori di età in base all'ordinamento del Paese di appartenenza o, comunque, in base alla legge italiana.

### **4) Categorie di dati oggetto di trattamento.**

Il trattamento può riguardare i soli dati e le sole operazioni che risultino indispensabili in relazione allo specifico profilo o alla personalità descritto o richiesto dalle persone interessate al matrimonio o alla convivenza.

I dati devono essere forniti personalmente dai medesimi interessati.

L'informativa preliminare al consenso scritto deve porre in particolare evidenza le categorie di dati trattati e le modalità della loro comunicazione a terzi.

### **5) Comunicazione dei dati.**

I dati possono essere comunicati nei limiti strettamente pertinenti all'esecuzione degli specifici incarichi ricevuti.

I titolari del trattamento, anche ai fini dell'eventuale comunicazione ad altri titolari delle modifiche apportate ai dati in accoglimento di una richiesta dell'interessato (art. 7, comma 3, lett. c), del Codice), devono conservare un elenco dei destinatari delle comunicazioni effettuate, recante un'annotazione delle specifiche categorie di dati comunicati.

L'eventuale diffusione anche per via telematica di taluni dati sensibili deve essere oggetto di apposita autorizzazione di questa Autorità.

### **6) Norme finali**

Restano fermi gli ulteriori obblighi previsti dalla legge e dai regolamenti, in particolare nell'ambito della legge penale e della disciplina di pubblica sicurezza, nonché in materia di tutela dei minori.

## **Capo VI - Prescrizioni comuni a tutti i trattamenti**

Per quanto non previsto dai capi che precedono, ai trattamenti ivi indicati si applicano, altresì, le seguenti prescrizioni:

### **1) Dati idonei a rivelare lo stato di salute**

Il trattamento dei dati idonei a rivelare lo stato di salute deve essere effettuato anche nel rispetto dell'autorizzazione n. 2/2004, rilasciata il 30 giugno 2004.

Il trattamento dei dati genetici non è consentito nei casi previsti dalla presente autorizzazione.

### **2) Modalità di trattamento**

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, dagli articoli 31 e seguenti del Codice e dall'Allegato B) al Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità indicate nei capi che precedono.

La comunicazione di dati all'interessato deve avvenire di regola direttamente a

quest'ultimo o a un suo delegato (fermo restando quanto previsto dall'art. 84, comma 1, del Codice), in plico chiuso o con altro mezzo idoneo a prevenire la conoscenza da parte di soggetti non autorizzati, anche attraverso la previsione di distanze di cortesia. Resta inoltre fermo l'obbligo di informare l'interessato, ai sensi dell'art. 13, commi 1, 4 e 5 del Codice, anche quando i dati sono raccolti presso terzi.

### **3) Conservazione dei dati**

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. e) del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità ovvero per adempiere agli obblighi o agli incarichi menzionati nei precedenti capi. A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per l'indispensabilità dei dati riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni e gli adempimenti.

Restano fermi i diversi termini di conservazione previsti dalle leggi o dai regolamenti. Resta altresì fermo quanto previsto nel capo II in materia di sondaggi e di ricerche.

### **4) Richieste di autorizzazione**

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.

Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.

Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

### **5) Norme finali**

Restano fermi gli obblighi previsti da norme di legge o di regolamento dalla normativa comunitaria, che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

a) dalla legge 20 maggio 1970, n. 300;

b) dalla legge 5 giugno 1990, n. 135;

Restano altresì fermi gli obblighi di legge che vietano la rivelazione senza giusta causa e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici, previsti anche dai codici deontologici e di buona condotta adottati in attuazione dell'art. 12 del Codice.

Resta ferma, infine, la possibilità di diffondere dati anonimi anche aggregati.

**6) Efficacia temporale e disciplina transitoria**

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2004 fino al 30 giugno 2005.

Qualora alla data della pubblicazione della presente autorizzazione il trattamento non sia già conforme alle prescrizioni non contenute nella precedente autorizzazione n. 5/2002, il titolare deve adeguarsi ad esse entro il 30 settembre 2004.

La presente autorizzazione sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana.<sup>11</sup>

Roma, 30 giugno 2004

---

<sup>11</sup> G.U. n. 190 del 14 agosto 2004



## **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.

Esame comparativo dei criteri di classificazione alberghiera, 1992

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

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

La prevenzione incendi: come gestire la sicurezza, 1995

Il Turismo nelle politiche strutturali della UE, 1995

Il franchising nel settore alberghiero, 1995

La prevenzione incendi: il registro dei controlli, 1996

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

Il collocamento obbligatorio nella giurisprudenza e nella prassi, 1998

Manuale di corretta prassi igienica per la ristorazione, 1998

Primo rapporto sul sistema alberghiero in Italia, 1999

Il codice del lavoro nel turismo, 1999 – 2003

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 nuovo collocamento dei disabili, 2001

Le stagioni dello sviluppo, 2001

Il nuovo contratto di lavoro a termine, 2001 –2002

Indagine sulla domanda turistica nei paesi esteri, 2001

Sistema ricettivo delle località termali in Italia, 2001

Terzo rapporto sul sistema alberghiero in Italia, 2002

I congedi parentali, 2002

Il turismo religioso in Italia, 2002

La privacy nell'ospitalità, 2002 - 2004

I condoni fiscali, 2003

Mercato del lavoro e professioni nel settore turismo, 2003

Le attività di intrattenimento negli alberghi, 2003

La nuova disciplina del lavoro extra, 2004

Dati essenziali sul movimento turistico nazionale ed internazionale, 2004

I contratti part-time nel settore turismo, 2004