IL CODICE SULLA PRIVACY
"TUTELA DELLE PERSONE E DI ALTRI SOGGETTI RISPETTO AL"
"TRATTAMENTO DEI DATI PERSONALI"
FASCICOLO DI FORMAZIONE

INDICE

Presentazione

Il decreto in esame (D. Lgs. 196 del 30 Giugno 2003, denominato anche Codice sulla privacy) sostituisce integralmente il D. Lgs. 675/96 e le sue successive modifiche e integrazioni, intervenute tra il 1997 e il 2003, armonizzandole e introducendo nuove regole e nuove sanzioni, garantendo *comunque* il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche nonché delle persone giuridiche e di ogni altro Ente o Associazione (con particolare riferimento alla riservatezza e all'identità personale).

Ambito di riferimento

Qualsiasi dato personale trattato o trattabile da chiunque nel territorio dello Stato Italiano.

Entrata in vigore

La Legge 675/96 era entrata in vigore l'8 Maggio 1997.

Il Codice sulla privacy è entrato in vigore dal 1° Gennaio 2004.

Principale normativa di riferimento

Legge 241 del 1990 e s.m.i.

D.P.R. 501 del 31 Marzo 1998

D.P.R. 318 del 28 Luglio 1999

D.P.R. 445 del 28 Dicembre 2000

D. Lgs. 196 del 30 Giugno 2003

Principali termini utilizzati dal Codice

- ✓ **<u>Trattamento</u>: qualunque operazione o complesso di operazioni - svolte con o senza l'ausilio di mezzi 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 personali (anche se non registrati in una banca dati); in particolare:**
  - **Registrazione: è l'atto di annotare o scrivere i dati trattati su registri a fini contabili, amministrativi e/o giuridici**
  - **Organizzazione: è l'atto di sistemare i dati trattati in base a esigenze di funzionalità e/o efficienza**
  - **Conservazione: è l'atto di custodire e archiviare i dati trattati**
  - **Modificazione: è l'atto di sottoporre a parziale trasformazione ovvero a mutamento i dati trattati, per lo più allo scopo di conseguire maggiore funzionalità e/o efficienza**
  - **Cancellazione: è l'atto di annullare, revocare e/o eliminare i dati trattati**
  - **Distruzione: è l'atto di "mandare al macero" documenti contenenti i dati trattati**
- ✓ **<u>Dato personale</u>: qualunque informazione relativa a una persona fisica o giuridica, a un Ente o a una Associazione (pubblici o privati) identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un codice o un numero di identificazione personale**
- ✓ **<u>Dati identificativi</u>: i dati personali che permettono l'identificazione diretta dell'interessato**
- ✓ **<u>Banca dati</u>: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti**
- ✓ **<u>Titolare</u>: la persona fisica o giuridica, la pubblica amministrazione o qualsiasi altro Ente, Associazione od organismo (pubblico o privato) cui competono le decisioni in ordine all'effettuazione, alle finalità e alle modalità del trattamento di dati personali, compreso il profilo della sicurezza. È titolare del trattamento l'entità nel suo complesso ovvero l'Ente/l'Associazione nella figura del legale rappresentante**

- ✓ **<u>Responsabile</u>: la persona fisica o giuridica, la pubblica amministrazione o qualsiasi altro Ente, Associazione od organismo (pubblico o privato) preposti dal Titolare del trattamento al trattamento di dati personali**
  - **Il Responsabile del trattamento, se designato (dal Titolare del trattamento), deve essere nominato tra soggetti che per esperienza, capacità e affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza**
  - **Il Responsabile del trattamento procede al trattamento attenendosi alle istruzioni impartite dal Titolare del trattamento il quale, anche per il tramite di verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni date e delle proprie istruzioni**
  - **Ove necessario per esigenze organizzative, possono essere designati Responsabili del trattamento più soggetti, anche mediante suddivisione di compiti**
  - **I compiti affidati al Responsabile del trattamento devono essere analiticamente specificati per iscritto dal Titolare del trattamento**
  - **I Responsabili del trattamento dei dati sono designati formalmente dal Titolare del trattamento**
  - **La designazione viene effettuata con lettera personale ai Responsabili del trattamento**
  - **Si provvede all'istruzione dei Responsabili del trattamento mettendo loro a disposizione:**
    - **la normativa vigente in materia e ogni eventuale o successiva integrazione o modificazione**
    - **il regolamento interno dell'entità di appartenenza**
    - **un fac-simile di informativa e uno schema per l'assunzione del consenso per il trattamento dei dati sensibili, qualora sia previsto dalla normativa vigente**
    - **la partecipazione ad appositi corsi di formazione**
- ✓ **<u>Incaricato</u>: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile del trattamento**
  - **In pratica, gli Incaricati del trattamento sono coloro che effettuano le operazioni di trattamento operando sotto la diretta autorità del Titolare del**

trattamento o del Responsabile del trattamento, attenendosi alle istruzioni impartite

- **La loro designazione viene effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito**

- ✓ **Interessato: la persona fisica o giuridica, l'Ente o l'Associazione o l'organismo (pubblici o privati) cui si riferiscono i dati personali**
- ✓ **Informativa: informazioni rese all'interessato al momento della raccolta dei dati personali**
- ✓ **Comunicazione: il dare conoscenza di 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**
- ✓ **Dato anonimo: il dato che, in origine o a seguito di trattamento, non può essere associato a un Interessato identificato o identificabile**
- ✓ **Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale**
- ✓ **Dati giudiziari: i dati personali idonei a rivelare provvedimenti giudiziari che si iscrivono nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti ovvero la qualità di indagato ai sensi degli Artt. 60 e 61 del codice di procedura penale**
- ✓ **Garante: l'autorità istituita ai sensi del D. Lgs. 675/96 e rimasta in carica anche con la promulgazione e l'entrata in vigore del Codice sulla privacy**

Attività interessate dal Codice

- ✓ **Il trattamento dei dati personali (con strumenti cartacei ed elettronici) e la sua notificazione (*ove del caso*)**
- ✓ **La comunicazione e la diffusione di dati personali**
- ✓ **La fornitura dell'informazione sul trattamento dei suoi dati all'Interessato; l'ottenimento del consenso e l'esercizio dei diritti da parte dell'Interessato**
- ✓ **Le disposizioni relative a specifici settori (ambito giudiziario, pubblico, sanitario, statistico e giornalistico; forze di polizia; difesa e sicurezza dello Stato; istruzione; sistemi previdenziali, bancari, finanziari e assicurativi; libere professioni e investigazione privata; giornalismo ed espressione letteraria ed artistica; marketing diretto)**

Notificazione del trattamento dei dati

Il Titolare del trattamento, qualora intenda procedere al trattamento di dati personali soggetti alle disposizioni del Codice sulla privacy e rientri nelle categorie previste dallo stesso, deve darne *obbligatoriamente* preventiva notifica in forma telematica all'Ufficio del Garante, qualora non lo abbia già fatto in forma cartacea/ informatizzata ai sensi del D. Lgs. 675/96.

Successive notificazioni si renderanno necessarie, sempre preventivamente, ogniqualvolta intervengano variazioni dei dati contenuti nelle notificazioni già fatte all'Ufficio del Garante.

Rammentiamo alcuni dati presenti nella notificazione:

- **Nome, denominazione o ragione sociale del Titolare del trattamento**
- **Domicilio, residenza o sede del Titolare del trattamento**
- **Finalità e modalità del trattamento**
- **Natura e luogo di custodia dei dati**
- **Categoria/e di Interessati**
- **Ambito di comunicazione e/o di diffusione dei dati**
- **Misure tecniche e organizzative adottate per la sicurezza**
- **Indicazione e dimensioni della/e banca/che-dati cui si riferisce il trattamento nonché l'*eventuale* connessione con altri trattamenti e/o banca/che-dati**
- **Nome o denominazione o ragione sociale - Domicilio o residenza o sede del Responsabile del trattamento**

- **Qualità e legittimazione del notificante**

Nota: nel caso di cessazione del trattamento, il Titolare del trattamento dovrà notificare al Garante la futura destinazione dei dati

Responsabilità del trattamento dei dati

L'*eventuale* nomina del Responsabile del trattamento è da effettuare per iscritto.

Le istruzioni per il trattamento dei dati personali debbono essere fornite per iscritto dal Titolare del trattamento al Responsabile del trattamento (*ove presente*) e da questi agli Incaricati.

La nomina, *ove del caso*, può riguardare più di un Responsabile del trattamento (*magari* suddividendo i compiti); l'*eventuale* suddivisione deve essere formalizzata per iscritto.

Particolari sui dati sensibili

Per il loro trattamento debbono essere richiesti:

- ✓ **il consenso scritto dell'Interessato (*quasi sempre! ...vedere nel seguito*)**
- ✓ **l'autorizzazione aprioristica del Garante (*ove del caso*)**

Questi dati possono concernere:

- ✓ **l'origine razziale e l'origine etnica**
- ✓ **le convinzioni religiose (evidenziate ad esempio dalle richieste di fruizione di permessi per festività religiose) e quelle filosofiche**
- ✓ **le opinioni politiche e/o l'adesione a organizzazioni e/o ad associazioni a carattere religioso/filosofico/politico/sindacale**
- ✓ **dati idonei a rivelare lo stato di salute, come: certificati di malattia, infortunio, inidoneità a particolari mansioni, maternità, appartenenza a categorie protette**
- ✓ **dati idonei a rivelare la vita sessuale**

…e: dati giudiziari!

Comunicazione e diffusione dei dati

<u>Premessa</u>

Alcuni dei casi in cui continuano a essere entrambe ammesse anche senza il consenso dell'interessato sono i seguenti:

- ✓ **se i dati provengono da pubblici registri, atti, elenchi, documenti accessibili a chiunque**

- ✓ **in adempimento a un obbligo previsto da Leggi, Regolamenti, Normative comunitarie, ecc.**
- ✓ **qualora i dati siano relativi allo svolgimento di attività economiche, nel rispetto delle vigenti Normative relative al segreto aziendale / industriale, …**

<u>Alcuni divieti alla comunicazione e alla diffusione</u>

Nessun dato può essere comunicato / diffuso in deroga alle finalità dichiarate, se ne sia stata ordinata la cancellazione o se sia decorso il periodo associato al trattamento previsto, consolidato all'atto della raccolta e successivamente notificato

<u>Comunicazione e diffusione di dati personali all'Estero</u>

Il trasferimento può avvenire previa notifica all'Ufficio del Garante

Il trasferimento viene *comunque* consentito, *tra l'altro*, qualora l'interessato abbia:

- ✓ **espresso per iscritto il proprio consenso nel caso dei dati cosiddetti "sensibili" o con preciso riferimento al codice di procedura penale**
- ✓ **espresso chiaramente il consenso in tutti gli altri casi**

Modalità di erogazione delle informazioni

Le informazioni all'Interessato o alla persona fornitrice dei dati sono da effettuare almeno oralmente ma preferibilmente per iscritto; tra queste vi sono:

- ✓ **le finalità delle raccolta e del successivo trattamento**
- ✓ **le modalità del trattamento**
- ✓ **la natura obbligatoria / facoltativa della fornitura**
- ✓ **le conseguenze *eventualmente* associate al rifiuto *eventuale* di fornire detti dati**
- ✓ **i soggetti / le categorie di soggetti cui i dati raccolti possono essere comunicati o di cui possono venire a conoscenza in qualità di Responsabili del trattamento ovvero Incaricati del trattamento e il relativo ambito di diffusione**
- ✓ **gli estremi identificativi del Titolare del trattamento e del/dei Responsabili del trattamento, indicando l'*eventuale* sito della rete di comunicazione ovvero le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato del/dei Responsabile/i del trattamento**
- ✓ **Il nome del Responsabile del trattamento dei dati quando sia stato designato un Responsabile per il riscontro all'Interessato in caso di esercizio dei diritti di cui all'Art. 7 del decreto in esame (e nel seguito di questo fascicolo, *cui si rinvia*)**

Anche se chi fornisce i dati è diverso dall'Interessato, le informazioni, in questo caso da fornire obbligatoriamente per iscritto, lo dovranno essere contestualmente all'atto della registrazione dei dati o, qualora sia prevista la comunicazione, non oltre la prima.

Questo adempimento non deve essere soddisfatto, *tra l'altro*, quando:

- ✓ **l'impiego di mezzi necessari viene dichiarato dall'Ufficio del Garante manifestamente sproporzionato rispetto al diritto tutelato, a fronte di richiesta scritta di giudizio formulata dal Titolare del trattamento**
- ✓ **l'adempimento viene riconosciuto "impossibile" da soddisfare, a giudizio dell'Ufficio del Garante, a fronte di richiesta scritta di giudizio formulata dal Titolare del trattamento, …**

Consenso al trattamento dei dati personali

- ✓ **I privati e gli enti pubblici economici possono trattare dati *abitualmente* previo consenso dell'Interessato; detto consenso è libero, specifico, revocabile *ma* da fornire o revocare per iscritto**

Esclusione del consenso al trattamento di dati personali

Il consenso non deve essere richiesto quando riguarda:

- ✓ **dati raccolti e detenuti in base a obblighi di Legge, Regolamenti, Normative comunitarie e/o per: soddisfare obblighi di contratto dei quali sia parte l'Interessato; acquisire informative precontrattuali attivate su richiesta dell'Interessato; adempiere a obblighi legali**
- ✓ **dati provenienti dai pubblici registri, elenchi, atti, documenti disponibili a chiunque**
- ✓ **dati anonimi da utilizzare per ricerche scientifiche e/o statistiche, …**

L'Interessato conserva, comunque, il diritto:

- ✓ **di avere accesso gratuito al Registro generale dei trattamenti (giacente c/o l'Ufficio del Garante)**
- ✓ **di essere informato in merito al Titolare del trattamento, al Responsabile del trattamento dei dati personali, ecc.**
- ✓ **di ottenere dal Titolare del trattamento (o dal Responsabile del trattamento) *sùbito*:**
    - **informazioni su dati che lo riguardano (registràti o meno)**

- **la cancellazione e/o la trasformazione in forma anonima o il blocco di dati personali trattati in violazione delle Leggi vigenti**
- **aggiornamenti, rettifiche, integrazioni, …**

Tutela dei diritti dell'interessato

Richiesta dell'Interessato

I diritti di cui all'Art. 7 sono esercitabili con richiesta rivolta senza formalità al Titolare del trattamento o al Responsabile del trattamento dei dati (anche per il tramite di un Incaricato), alla quale deve essere fornito idoneo riscontro senza ritardo.

La richiesta può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica.

Quando riguarda l'esercizio dei diritti di cui all'Art. 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e, in tal caso, deve essere annotata sinteticamente a cura del Responsabile del trattamento o di un Incaricato.

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.

Nota: i diritti di cui all'Art. 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.

Verifica dell'identità dell'Interessato

L'identità dell'Interessato deve essere 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.

Riscontro all'Interessato

Per garantire l'effettivo esercizio dei diritti di cui all'Art. 7 il Titolare del trattamento è tenuto:

a) ad agevolare l'accesso ai dati personali da parte dell'Interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati a 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.

I dati sono estratti a cura del Responsabile del trattamento o di 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. Se vi è richiesta specifica da parte dell'Interessato, si provvede alla trasposizione dei dati su supporto cartaceo o informatico ovvero alla loro trasmissione per via telematica.

Quando, a seguito della richiesta di cui all'Art. 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; il contributo di cui al comma 7 non può comunque superare l'importo determinato dall'Ufficio del Garante con provvedimento di carattere generale, *cui si rinvia*.

<u>Esercizio dei diritti dell'Interessato</u>

I diritti di cui all'Art. 13 / comma 1 del D. Lgs. 675/96, recepiti interamente dal Codice sulla privacy (Art. 7), possono essere fatti valere di fronte all'autorità giudiziaria o con ricorso all'Ufficio del Garante; la prima alternativa, *se precedente*, esclude la seconda.

L'Ufficio del Garante può:

- ✓ **non pronunciarsi sul ricorso: equivale a rigetto a partire da 20 (venti) giorni dopo la presentazione del ricorso,**
- ✓ **pronunciarsi sul ricorso, emanando un provvedimento.**

Qualora esso sia provvisorio, cessa di avere effetto dopo 20 (venti) giorni dalla sua emanazione qualora l'Ufficio del Garante, nel frattempo, non si sia definitivamente pronunciato sul ricorso con provvedimento definitivo.

L'opposizione al Tribunale può avvenire, a cura del Titolare del trattamento o dell'Interessato, entro 30 (trenta) giorni dalla data di comunicazione del provvedimento o del rigetto (tacito), pur non sospendendosi l'applicazione del provvedimento, qualora ancora in vigore.

È il Tribunale che decide; avverso un suo decreto è ammesso solo il ricorso per Cassazione.

In generale, tutte le controversie sono di competenza dell'autorità giudiziaria ordinaria.

Ufficio del Garante

L'Ufficio del Garante è un organo collegiale composto da quattro membri, eletti due dalla Camera dei deputati e due dal Senato della Repubblica, di cui uno viene eletto Presidente e ha voto prevalente in caso di parità.

Essi sono e dovranno sempre essere esperti di riconosciuto valore nei settori del diritto e/o della informatica, durano in carica 4 anni (…e non avrebbero potuto essere rieletti più di una volta …ma lo sono stati).

I principali compiti dell'Ufficio del Garante:

- ✓ **Istituire e manutenere un Registro generale dei trattamenti sulla base delle notificazioni ricevute**
- ✓ **Verificare che i trattamenti siano effettuati nel rispetto di Leggi e Regolamenti e in conformità alle notificazioni**
- ✓ **Segnalare tempestivamente le modifiche conseguenti a variazioni delle disposizioni del Codice sulla privacy**
- ✓ **Gestire i reclami e i ricorsi, adottando, *ove del caso*, provvedimenti acconci**
- ✓ **Vigilare sui casi di cessazione del trattamento**
- ✓ **Denunciare i fatti configurabili come reati perseguibili d'ufficio**
- ✓ **Promuovere la sottoscrizione dei codici di deontologia professionale per le categorie interessate**
- ✓ **Divulgare fra il pubblico norme e finalità del Codice**
- ✓ **Segnalare al Governo *eventuali* necessità di variazioni ed essere consultato nella fase di studio di dette variazioni**

Sicurezza dei dati

<u>Azioni di custodia e controllo</u>

Allo stato attuale delle cose sono definite "necessarie" e "dovute" azioni che garantiscano custodia / controllo tali da ridurre al minimo i rischi di: distruzione o perdita (*anche accidentale*) dei dati; accesso non autorizzato; trattamento non consentito o non conforme alle finalità notificate della raccolta

Esempi di comunicazioni:

Nomina del Responsabile del trattamento dei dati

Nomina dell'Incaricato (al trattamento dei dati)

Delega al trattamento operativo dei dati

Notificazione, *ove del caso*, all'Ufficio del Garante del trattamento di dati e della cessazione del trattamento di dati

Informativa iniziale all'Interessato o a chi ne fa le veci (formula generalizzata)

Informativa iniziale all'Interessato (formula per i dipendenti/equipollenti e i candidati all'assunzione)

Consenso al trattamento di dati personali/sensibili da parte dell'Interessato o di persona da lui delegata

Consenso alla comunicazione e/o diffusione di dati personali/sensibili da parte dell'Interessato o di persona da lui delegata

<u>Misure di sicurezza</u>

Obblighi di sicurezza:

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.

Misure minime di sicurezza:

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

Trattamenti con strumenti elettronici:

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) del decreto qui in esame (*si veda nel seguito*), le seguenti misure minime:

- **autenticazione informatica;**
- **adozione di procedure di gestione delle credenziali di autenticazione;**
- **utilizzazione di un sistema di autorizzazione;**
- **aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;**

- **protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;**
- **adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;**
- **tenuta di un aggiornato Documento Programmatico sulla Sicurezza dei dati personali (D.P.S.) (obbligo decaduto alla data);**
- **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.**

Trattamenti senza l'ausilio di strumenti elettronici:

Il trattamento dì 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) del decreto in esame (si veda nel seguito), le seguenti misure minime:

- **aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati o alle unità organizzative;**
- **previsione di procedure per un'idonea custodia di atti e documenti affidati agli Incaricati per lo svolgimento dei relativi compiti;**
- **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.**

Cenni sul Disciplinare Tecnico [in materia di misure minime di Sicurezza (Artt. da 33 a 36 del Codice sulla privacy)]

<u>Trattamenti con strumenti elettronici:</u>

Sistema di autenticazione informatica:

- **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.**
- **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 i identificativo o a una parola chiave.

- **A ogni Incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.**
- **Con le istruzioni impartite agli Incaricati deve essere prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso e uso esclusivo dell'Incaricato medesimo.**
- **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.**
- **Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri Incaricati, neppure in tempi diversi.**
- **Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.**
- **Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali.**
- **Devono infine essere impartite istruzioni agli Incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.**

Principali novità armonizzate nel Codice sulla privacy - 1

Riorganizzazione dell'Ufficio del Garante

Il 19 febbraio 1999 si deliberò di raddoppiare l'organico dell'Ufficio del Garante, consentendo all'ufficio dell'autorità sulla *privacy* di passare da ca. 50 a ca. 100 unità.

Di queste, alcune hanno assunto la veste di ufficiale o agente di polizia giudiziaria, così che l'*eventuale* rifiuto del Responsabile del trattamento o del Titolare del trattamento di dati personali a fornire collaborazione a fronte di richieste di accertamenti, ispezioni, controlli vari formulate dall'Ufficio del Garante possa prefigurare un'*eventuale* denuncia per resistenza a pubblico ufficiale.

Questa particolare qualifica attribuita agli ispettori delegati dall'Ufficio del Garante consente loro di effettuare, oltre a verifiche di tipo amministrativo, accertamenti in merito a violazioni di natura diversa (ad esempio: l'*eventuale* trattamento illecito di dati personali relativi a minori, ecc.).

Questi accertamenti, anche ai sensi delle modifiche apportate dal D.P.R. 501 del 31 Marzo 1998, possono essere effettuati da detti ispettori, *ove del caso assistiti da consulenti specialisti e/o da altri organi dello Stato*, sempre e solo su autorizzazione del Presidente del Tribunale avente giurisdizione sul Titolare del trattamento interessato all'accertamento.

L'accertamento può avere inizio dopo le ore 7 e non dopo le ore 20, senza o con preavviso (verbale o scritto).

L'accertamento può essere effettuato senza la preventiva autorizzazione del Presidente del Tribunale avente giurisdizione solo qualora vi sia l'assenso scritto e informato del Titolare del trattamento o del Responsabile del trattamento.

In caso di rifiuto da parte del Titolare del trattamento o del Responsabile del trattamento a fornire una risposta, vigono le sanzioni riportate nel testo del D. Lgs. 675/96 riprese …e "appesantite" dal Codice sulla privacy.

Con l'ufficializzazione del regolamento per l'organizzazione e il funzionamento dell'Ufficio del Garante si è colta anche l'occasione per sottolineare la necessità di offrire la massima tutela agli Interessati al trattamento dei dati, dando maggiore enfasi ai diritti di questi ultimi in merito alla possibilità loro offerta di richiedere a qualsiasi Titolare del trattamento e/o Responsabile del trattamento di dati personali informazioni precise e incontestabili sulla tipologia dei dati che li riguardano e da

questi ultimi detenuti e sulle modalità di trattamento adottate per garantirne la sicurezza ai sensi delle disposizioni legislative che tutelano i dati personali.

***In estrema sintesi*: nessun Titolare del trattamento potrà rifiutarsi di fornire una risposta tempestiva ed esaustiva a fronte di richieste verbali o scritte da parte di qualsiasi Interessato, potendo, in cambio, richiedere solo una piccola tassa per la ricerca (regolamentata, ma comunque sino a un massimo prestabilito qualora la stessa sia negativa (*)) e fornendo, in caso contrario, un servizio totalmente gratuito.**

(*): si intende con ciò la rilevazione – incontestabile – e la conferma (scritta, ove richiesto) da parte del Titolare del trattamento o del Responsabile del trattamento, che nessun dato personale del postulante è dallo stesso detenuto.

In caso di rifiuto da parte del Titolare del trattamento o del Responsabile del trattamento a fornire una risposta, scattano le sanzioni in vigore alla data.

Anche in merito ai ricorsi di cui all'Art. 29 del D. Lgs. 675/96 il regolamento successivamente emesso dall'Ufficio del Garante e recepito dal Codice sulla privacy fornisce maggiori delucidazioni rispetto al mero testo di legge; in particolare in merito ai loro contenuti, alle clausole di inammissibilità e al procedimento che i medesimi generano.

<u>Contenuti dei ricorsi all'Ufficio del Garante</u>

Nome, denominazione o ragione sociale, domicilio o residenza o sede del ricorrente (corredati di un recapito, di un numero telefonico e/o di fax per facilitare l'*eventuale* prosecuzione del rapporto) e del Titolare del trattamento o dell'*eventuale* Responsabile del trattamento

Nome dell'*eventuale* procuratore speciale e indicazioni sul domicilio eletto dallo stesso

Indicazione del provvedimento richiesto, con evidenza della data della richiesta al Titolare del trattamento o all'*eventuale* Responsabile del trattamento e degli elementi che giustificavano la domanda …e il conseguente ricorso a fronte della mancata risposta

Firma/e di sottoscrizione del ricorrente (e dell'*eventuale* procuratore); *…tra gli allegati si rammentano invece: eventuale* procura, copia della domanda posta al Titolare al trattamento o al Responsabile del trattamento, prova del versamento effettuato dei diritti di segreteria e tutta l'*eventuale* documentazione reputata utile per una corretta valutazione del ricorso

Fatte salve le clausole d'inammissibilità riportate nel testo del D. Lgs. 675/96 e interamente recepite dal Codice sulla privacy, il procedimento adottato comporta l'assunzione in prima persona del ruolo di giudice e di moderatore da parte dell'Ufficio del Garante, che richiede innanzitutto al Titolare del trattamento o al Responsabile del trattamento di soddisfare la domanda del ricorrente.

Qualora ciò si verifichi e il ricorrente ne abbia espressamente fatta richiesta, il Titolare del trattamento dovrà sopportare ogni *eventuale* costo sopportato dal ricorrente per operare il ricorso.

In caso di prosecuzione del rifiuto, l'azione si svilupperà analogamente a una causa giudiziale, con la presentazione di memorie, documenti, …; l'*eventuale* richiesta di intervento periziale; un possibile contraddittorio; la decisione, assunta dall'Ufficio del Garante anche in merito agli oneri connessi al procedimento ...e l'attuazione delle decisioni a cura dell'Ufficio del Garante o di altro organo dello Stato a ciò delegato.

Le decisioni dell'Ufficio del Garante possono essere impugnate solo rivolgendosi all'autorità giudiziaria!

Le principali novità armonizzate nel Codice sulla privacy - 2

<u>Obbligo di produrre e aggiornare il D.P.S.</u> (decaduto alla data)

Si tratta del Documento Programmatico sulla Sicurezza (D.P.S.) previsto dall'Art. 6 "Regolamento sulle misure minime di sicurezza" del D.P.R. 28 Luglio 1999, n. 318 e recepito dal Codice sulla privacy.

Questo documento intendeva definire formalmente, sulla base di un'adeguata "analisi dei rischi" e della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati medesimi, quanto segue:

- ✓ **i criteri tecnici e organizzativi adottati per proteggere aree e locali interessati dalle misure di sicurezza e le procedure adottate per controllare l'accesso delle persone autorizzate alle aree/ai locali medesime/i**
- ✓ **i criteri e le procedure adottati/e per assicurare l'integrità dei dati**
- ✓ **i criteri e le procedure adottati/e per garantire la sicurezza della trasmissione dei dati (comprese quelli/e adottati/e per *restringere* gli accessi per via telematica)**
- ✓ **i piani di formazione di tutti gli incaricati del trattamento (Responsabile/ Incaricati), al fine di renderli adeguatamente edotti in merito ai criteri e alle procedure adottati/e per prevenire danni associati ai rischi individuati**

L'obiettivo finale era di garantire non solo l'introduzione e la conservazione, oltre al possibile miglioramento, delle misure minime di sicurezza dei dati di cui al D.P.R. sopra citato, *ma* di misure "idonee" a offrire garanzie "certe" in merito alla sicurezza medesima.

Questo documento doveva essere rivisto e aggiornato, a cura di un Esperto della materia, con frequenza annuale ed entro ogni 31 Marzo, a seguito di:

- ✓ **una puntuale verifica dell'efficacia delle misure adottate**
- ✓ **l'*eventuale* decisione in merito all'attivazione di processi correttivi e/o preventivi e/o di miglioramento continuo**

…ambedue comunque documentate con l'emissione di apposito verbale.

Nel caso di strutture certificate ai sensi della Norma ISO 9001:2008 questo documento, di fatto, assumeva la veste di *input* a uno dei riesami della Direzione, nella fase di analisi e consolidamento delle misure da adottare per garantire un miglioramento continuo.

Le principali novità armonizzate nel Codice sulla privacy - 3

<u>Sanzioni in cui incorreva chi trasgrediva</u>

Per danni cagionati per effetto del trattamento di dati personali: essi erano risarciti ai sensi dell'Art. 2050 del codice civile

Per omessa, intempestiva o infedele notificazione:

- **1° caso: notificazione/i di trattamento/i sia in Italia sia all'Estero: da tre mesi a due anni**
- **2° caso: notificazione della cessazione di trattamento/i: sino a un anno**

Per trattamento illecito di dati personali:

- ✓ **In violazione a quanto disposto dagli Artt. 11, 20 e 27: sino a due anni**
- ✓ **nel caso di comunicazione o diffusione di dati personali in violazione a quanto disposto dagli Artt. 11, 20 e 27: da tre mesi a due anni**
- ✓ **nel caso di comunicazione o diffusione di dati personali in violazione a quanto disposto dagli Artt. 21, 22, 23 e 24 ovvero del divieto di cui all'Art. 28 / comma 3 del D. Lgs. 675/96: da tre mesi a due anni**

Nota: se inoltre ne derivava nocumento, la reclusione era da uno a due anni.

Per omessa adozione delle misure minime di sicurezza:

Violazione ai commi 2/3 Art.15: sino a un anno

Se ne derivava anche nocumento: da due mesi a due anni

Se il fatto era commesso per colpa: sino a un anno

Il ravvedimento operoso, previa attuazione di dette misure, consentiva di depenalizzarsi, pagando una somma compresa tra i 5.164,00 e i 41.316,00 Euro

Per inosservanza dei provvedimenti dell'Ufficio del Garante:

- ✓ **Violazione ai sensi dell'Art. 22 / comma 2 o dell'Art. 29 / commi 4 e 5: da tre mesi a due anni**

Sanzioni amministrative:

- ✓ **Per omissione nella fornitura delle informazioni o nell'esibizione dei documenti richiesti dall'Ufficio del Garante: sino a 15.493,00 Euro**
- ✓ **Per violazione delle disposizioni con mancata informativa all'Interessato o a chi forniva i dati al momento della raccolta: da 9.296,00 a 15.493,00 Euro**
- ✓ **Per omessa, intempestiva o infedele notificazione: da 5.164,00 a 30.987,00 Euro**

Sanzioni in cui incorre chi trasgredisce

- ✓ **Per inidonea o omessa informativa all'Interessato: da € 5.000 a € 30.000,00**
- ✓ **Per danni cagionati per effetto del trattamento di dati personali: risarcibili ai sensi dell'Art. 2050 del codice civile**
- ✓ **Per omessa o intempestiva ovvero infedele notificazione: da € 10.000,00 a € 60.000,00 e da 6 mesi a 3 anni**
- ✓ **Per omessa adozione delle misure minime di sicurezza dei dati: da € 10.000,00 a € 50.000,00**
- ✓ **Per inosservanza dei provvedimenti dell'Ufficio del Garante: da € 4.000,00 a € 24.000,00 e da 3 mesi a 2 anni**

Varianti introdotte negli ultimi anni

L'Ufficio del Garante ha prodotto nel tempo numerose circolari, comunicando:

- ✓ **l'attuazione del sistema sanzionatorio senza alcuna esclusione;**
- ✓ **l'obbligo di continuare a somministrare l'informativa a tutte le persone fisiche di cui si detengano dati personali e gli incarichi al trattamento dei dati a tutti coloro che per ragioni di lavoro trattano dati personali (propri e) di altri;**
- ✓ **l'interruzione dell'obbligo di produrre annualmente, entro il termine del 31 Marzo, il Documento Programmatico sulla Sicurezza dei dati personali (D.P.S.);**
- ✓ **l'interruzione dell'obbligo di aggiornare annualmente (formazione continua) il personale dell'entità interessata che abbia già partecipato a corsi di formazione ex-novo o in aggiornamento;**
- ✓ **l'obbligo di continuare a formare tutto il personale neo-inserito ovvero il personale già in carico che non abbia ancora partecipato a corsi di formazione in materia di privacy.**

Conclusioni

Fermo restando il suggerimento di leggere i testi delle variazioni intervenute e, in particolare, una "versione per il pubblico" del Codice sulla privacy, com'è il presente fascicolo, qui si vuole sottolineare che le variazioni e integrazioni apportate alle modalità di cui al D. Lgs. 675/96 e riviste e armonizzate nel testo del Codice sulla privacy non sono esigue e si presentano, talvolta, di non semplice applicazione.

Appendice

Conservazione delle cartelle cliniche

RIFERIMENTI NORMATIVI

Costituzione italiana Art. 97

D.P.R. 27 Marzo 1969 numero 128 Art. 7

D.P.R. 14 Marzo 1974 numero 225

D.P.R. 27 Marzo 1969 numero 128 Artt. 2 - 5

Nuovo codice di deontologia medica Art.10

Circolare Ministero della sanità 19 Dicembre 1986

Le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente, poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario.

La documentazione diagnostica assimilabile alle radiografie va conservata almeno 20 (venti) anni.

È prevista la possibilità della microfilmatura:

- **Legge 4 Gennaio 1968 numero 15**
- **D.p.c.m. 11 Settembre 1974**
- **Decreto Ministro per i Beni culturali e ambientali 29 Marzo 1979**
- **D.P.R. 28 Dicembre 2000 numero 445**