Fondazione Luca Pacioli

CODICE DELLA PRIVACY

TESTO UNICO IN MATERIA DI DATI PERSONALI

(D.Lgs. 30 giugno 2003, n. 169)

Documento n. 9 del 19 marzo 2004

CIRCOLARE

Via G. Paisiello, 24 – 00198 Roma – tel.: 06/85.440.1 (fax 06/85.440.223) – C.F.:80459660587
www.fondazionelucapacioli.it - fondazionelucapacioli@consrag.it

INDICE

CODICE DELLA PRIVACY – TESTO UNICO IN MATERIA DI DATI PERSONALI

(D.Lgs. 30 giugno 2003, n. 169)

Dal 1° gennaio 2004 è entrato in vigore il Codice della Privacy. La nuova disciplina oltre a raccogliere in un unico contesto semplificato le molte disposizioni previgenti, introduce una serie di modificazioni volte da un lato a semplificare gli adempimenti previsti in materia di informativa, consenso e notificazione, dall'altro a prescrivere l'adozione di nuove misure minime di sicurezza, specialmente in ambito informatico.
La disciplina dovrà essere applicata da tutti coloro che trattino dati personali e, in tale ambito soggettivo, sono compresi anche i professionisti. Si richiama subito l'attenzione sul fatto che taluni adempimenti andranno assolti in termini brevi, onde non incorrere nelle pesanti sanzioni previste dalla nuove normativa.
Con la presente circolare si intende fornire una prima illustrazione dei contenuti del nuovo Testo Unico. La materia presenta allo stato profili di dubbia interpretazione che la Fondazione Luca Pacioli ha provveduto a rappresentare all'Autorità Garante per la protezione dei dati personali per ottenere un sollecito chiarimento. Si fa pertanto riserva di tornare sull'argomento qualora intervenissero novità.

Introduzione

Dal 1° gennaio 2004 è entrato in vigore il Codice della Privacy. Si tratta di un Testo Unico sulle disposizioni in materia di protezione dei dati personali, che è stato adottato con il d.lgs. 30 giugno 2003, n. 196, pubblicato in Gazzetta Ufficiale il 29 luglio 2003.
Tale decreto è stato emanato ai sensi della legge di delega 24 marzo 2001, n. 127, la quale, all'art. 1, ha previsto che "Il Governo emana un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni connesse coordinandovi le norme vigenti ed apportando alle medesime le integrazioni e modificazioni necessarie al predetto coordinamento o per assicurarne la migliore attuazione."
Il testo unico riordina tutta la normativa in tema di trattamento dei dati personali riunendo in un unico contesto la L. 675/1996 e gli altri decreti legislativi[1], regola-

1 D.Lgs. n. 123 del 9 maggio 1197, D.Lgs. n. 255 del 28 luglio 1997, D.Lgs. n. 135 dell'8 maggio 1998, D.Lgs. n. 171 del 13 maggio 1998, D.Lgs. n. 389 del 6 novembre 1998, D.Lgs. n. 51 del 26 febbraio 1999, D.Lgs. n. 135 dell'11 maggio 1999, D.lgs. 281 del 30 luglio 1999, D.Lgs. n. 282 del 30 luglio 1999, D.Lgs. n. 467 del 28 dicembre 2001.

menti e codici deontologici che si sono succeduti in questi ultimi anni, apportando numerose integrazioni e modificazioni che tengono conto della "giurisprudenza" del Garante per la protezione dei dati personali e della direttiva Ue 2000/58 sulla riservatezza nelle comunicazioni elettroniche.
Nell'opera di sistematizzazione dell'intera disciplina, il Legislatore si è ispirato ai principi di semplificazione ed efficacia, riducendo del 30% circa (come rileva la relazione di accompagnamento al codice) il numero di disposizioni vigenti in materia. In particolare, l'opera di semplificazione ha investito principalmente l'adempimento delle notificazioni, dell'informativa e del consenso con un conseguente snellimento degli adempimenti necessari.

Il codice, costituito da 186 articoli, si compone di tre parti che contengono rispettivamente:

- disposizioni generali (artt. 1-45), riguardanti le regole "sostanziali" della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, salvo eventuali regole specifiche (II parte);
- disposizioni particolari (artt. 46-140) per specifici trattamenti, ad integrazione od eccezione alle disposizioni generali (I parte);
- disposizioni (artt. 141-186) relative alle azioni di tutela dell'interessato ed al sistema sanzionatorio cui si aggiungono le norme di modifica, finali e di carattere transitorio.

Il codice è completato da tre allegati:

- Allegato A: codici di deontologia;
- Allegato B: disciplinare tecnico in materia di misure minime di sicurezza;
- Allegato C: elenco dei trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia che dovranno essere individuati entro il 30 giugno 2004 dai Ministeri competenti.

PARTE I
Disposizioni generali

1. Diritto alla protezione dei dati personali

Diversamente dal passato, il "Codice" definisce il diritto alla protezione dei dati personali come un vero e proprio diritto della persona: l'art. 1, infatti, prevede espressamente che "Chiunque ha diritto alla protezione dei dati personali". In tal modo, così come i tradizionali diritti della personalità (nome, immagine, riservatezza) anche il diritto di ogni soggetto, sia esso persona fisica o giuridica, alla protezione dei dati personali viene ad essere tutelato direttamente dalla legge. Il principio riproduce quasi fedelmente l'art. 8 della Carta dei diritti fondamentali dell'Unione Europea stipulata a Nizza il 7 dicembre 2000 "Chiunque ha diritto alla protezione dei dati personali che lo riguardano."

2. Tipologia dei dati oggetto di tutela

Il testo unico riproduce la distinzione principale, già evidenziata dalla legge n. 675/96, tra dati ordinari e dati sensibili. Sono dati sensibili, a norma dell'art. 4, lett. d), testo unico privacy, "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale." I dati che non rientrano in questa definizione vengono ritenuti dati "ordinari". Viene inoltre mantenuta la nozione di dati "giudiziari" aggiornata tecnicamente a seguito dell'adozione del testo unico in materia di casellario giudiziario.

E' possibile rilevare un'ulteriore categoria di dati laddove, all'art. 17 del d.lgs. 196/2003, viene previsto che "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.". Recependo una norma introdotta dal d.lgs. 467/01 viene quindi mantenuta tale categoria che può essere considerata "intermedia" tra quella dei dati ordinari e dati sensibili. Sarà cura del Garante dettare gli accorgimenti necessari per il trattamento di tale tipologia di dati.

3. Modalità del trattamento dati

La modalità di trattamento dati rimane invariata rispetto alla precedente disciplina, stabilita dall'art. 9 della legge 675/96, che viene riprodotto pressoché integralmente nel nuovo art. 11 del d.lgs. 196/93.
I dati personali oggetto di trattamento devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- 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.

I dati personali che non vengono trattati in conformità a tale disciplina non possono essere utilizzati.

4. Informativa alla Privacy

Rimane confermato, ai sensi dell'art. 13 del d.lgs. 196/03, l'obbligo di informativa nei confronti dell'interessato che fornisca i propri dati personali sulle finalità e modalità del trattamento dati, sulla natura obbligatoria o facoltativa del conferimento dati, sulle conseguenze di un eventuale rifiuto a fornire dati, sull'eventuale comunicazione dei dati ai terzi ed il loro ambito di diffusione. Inoltre, l'interessato, deve essere informato sul diritto di accesso ai dati che lo riguardano, cioè sulla possibilità di ottenerne l'aggiornamento, la rettifica, l'integrazione o la cancellazione (art. 7 d.lgs. 196/03).

5. Consenso al trattamento dati

Successivamente alle informazioni ricevute sui propri diritti, affinchè i dati possano essere trattati lecitamente, è necessario che l'interessato fornisca il proprio consenso, documentato per iscritto nel caso dei dati personali, e manifestato in forma scritta per i dati sensibili, a norma dell'art. 23 del d.lgs. 196/03.
L'art. 24 del d.lgs. 196/03 riporta con precisione le ipotesi in cui può essere effettuato il trattamento dei dati senza che sia necessario prestare consenso. Tra queste quelle principali sono:

- i casi previsti nella II parte del testo unico (disposizioni relative a specifici settori);

- quando il trattamento sia necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- quando il trattamento sia 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 delle attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale.

6. Autorizzazione al trattamento dati

Successivamente al consenso, nel caso in cui vengano trattati dati sensibili, è necessaria l'autorizzazione del Garante (art. 26, d.lgs. 196/03). Il Garante comunica la propria decisione in merito alla richiesta di autorizzazione al trattamento entro 45 giorni, decorsi i quali la domanda si considera rigettata. Contestualmente alla concessione dell'autorizzazione il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.
L'autorizzazione da parte del Garante non è necessaria nei seguenti casi:

- trattamento dati relativi agli aderenti alle confessioni religiose, effettuato dagli organi religiosi ovvero da enti civilmente riconosciuti; sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni;
- trattamento dati riguardanti l'adesione di associazioni o organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

7. Titolare, responsabile e incaricati del trattamento dati

Ai fini del codice privacy, viene ritenuto titolare del trattamento (art. 28) l'entità nel suo complesso (persona giuridica, pubblica amministrazione, ente associazione od organismo) che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, compreso il profilo della sicurezza. Il titolare del trattamento, facoltativamente, può designare uno o più responsabili (art. 29) a cui affidare compiti stabiliti per iscritto. Da ultimo il legislatore individua un'altra figura, anch'essa facoltativa, nell'incaricato del trattamento (art. 30) che potrà effettuare le operazioni di trattamento dati solo ed esclusivamente sotto la diretta autorità del titolare e del responsabile.

8. Obblighi e misure di sicurezza

Particolarmente stringenti risultano le nuove misure di sicurezza, poste a tutela dei dati personali, stabiliti dal Testo Unico.
Innanzitutto l'art. 31 individua gli obblighi di sicurezza a carico del titolare del trattamento in una generale indicazione di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati sottoposti a trattamento.
Più specificamente, al capo II, del titolo V, artt. 33, 34, 35, 36, vengono stabilite nel dettaglio le misure minime di sicurezza che è necessario adottare al fine di assicurare un livello minimo di protezione dei dati. In caso di trattamenti effettuati attraverso l'ausilio di strumenti elettronici vengono prescritte (art. 34) le seguenti misure minime di sicurezza:

- 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 (v. capitolo successivo);
- 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.

Viceversa, per quanto riguarda il trattamento di dati personali effettuato senza il ricorso a strumenti elettronici, le misure minime di sicurezza devono essere adottate nei modi previsti dall'allegato b) del T.U. (disciplinare tecnico in materia di misure minime di sicurezza) e concernono (art. 35):

- 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.

Da ultimo va segnalato che il disciplinare tecnico in materia di misure minime di sicurezza (allegato b)), viene 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.

9. Notificazione al Garante

La notificazione al Garante è l'atto con cui l'impresa, il professionista o la pubblica amministrazione segnala al Garante i trattamenti di dati che si intendono effettuare. Il codice della privacy semplifica notevolmente le procedure legate all'assolvimento di tale onere. Innanzitutto, viene capovolta l'impostazione della l. 675/96 e sue successive modifiche, con la quale erano obbligati a notificare tutti i soggetti non esplicitamente esentati dalla norma. L'art. 37 del codice, al contrario, identifica esclusivamente i casi in cui la notifica deve essere effettuata, limitando l'onere a particolari casi di trattamento di dati sensibili (specie se sanitari) con determinate modalità d'uso, di dati trattati con l'ausilio di strumenti elettronici volti alla profilazione dei consumatori, o in relazione a procedure di selezione del personale e ricerche di marketing, nonché in ipotesi di utilizzo di informazioni commerciali e relative alla solvibilità.

Vengono inoltre semplificate le modalità di notificazione, l'art. 38, infatti, prevede che la notificazione sia validamente effettuata solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le modalità da questi impartite per quanto riguarda la sottoscrizione con firma digitale. Il modello per la notificazione al Garante è disponibile al sito internet https://web.garanteprivacy.it/rgt/NotificaTelematica.php.
Si ricorda che i termini per la trasmissione per via telematica della notifica sono i seguenti:

- entro il 30 aprile 2004 per le attività che erano già in essere prima del 1° gennaio 2004;
- prima che inizi il trattamento per quelle attività di trattamento dati che non esistevano prima del 1° gennaio 2004.

PARTE II

Le regole e gli adempimenti per i professionisti

1. Ambito soggettivo di applicazione

Devono adeguarsi al nuovo Testo unico sulla privacy tutti coloro che trattano dati personali: aziende, professionisti, cooperative, associazioni, pubbliche amministrazioni, scuole, comuni, ospedali, ecc..

2. Adempimenti

I professionisti e le aziende che si trovino a trattare dati personali, per adeguarsi alla nuova normativa in tema di privacy, hanno l'obbligo di mettersi in regola attraverso alcuni accorgimenti.

1 Nomina delle figure previste dalla legge: Titolare e Responsabile del trattamento; si ricorda che titolare e responsabile possono essere la stessa persona.
2 Sistemi di protezione informatica (antivirus, firewall) per proteggere gli elaboratori dal rischio di intrusione e di virus.
3 Procedure per la tutela e la riservatezza dei dati in tutte le fasi del trattamento (raccolta, registrazione, correzione, trasmissione, distruzione,...)
4 Misure fisiche idonee alla protezione dei locali in cui vengono conservati i dati (allarmi antifurto, limitazione degli accessi ai locali, armadi con lucchetti...)
5 Ogni accorgimento utilizzato ai fini della tutela dei dati personali deve essere rigorosamente documentato nel DPS (Documento Programmatico sulla sicurezza). Solamente la redazione del DPS fa prova dell'avvenuto adeguamento alla normativa.

3. Il Documento Programmatico sulla Sicurezza (DPS)

Una delle misure di sicurezza, ai sensi dell'art. 34 e dell'allegato b) punto 19 del Codice privacy è l'obbligo di redazione di un Documento Programmatico sulla Sicurezza (DPS).
Non risulta agevole delimitare l'ambito di applicazione della norma: chi, cioè, in concreto, sia obbligato alla redazione del documento. L'art. 34 del codice lett. g),

prevede che, tra le misure minime da adottare nel trattamento di dati personali con strumenti elettronici, sia prevista la redazione del DPS. All'art. 35 in materia di misure minime di sicurezza per i trattamenti effettuati senza l'ausilio di strumenti elettronici, invece, non è fatta menzione di questo adempimento. Dalla comparazione delle due norme si può dunque desumere che la redazione del DPS sia obbligatoria esclusivamente per chi tratti dati personali (di qualsiasi natura) con l'ausilio di strumenti informatici. L'allegato b) del codice al punto 19, conferma l'obbligo della redazione del DPS per i trattamenti effettuati mediante l'ausilio di strumenti elettronici ma limita l'onere al caso di trattamento di dati sensibili o giudiziari. Difficile a questo punto, stabilire se l'adempimento sia richiesto per il trattamento di dati personali di qualsiasi natura od esclusivamente per quella più limitata categoria dei dati sensibili e giudiziari. Sembra fin qui potersi affermare solo l'esenzione dell'incombenza da parte di chi non tratti i dati con l'ausilio degli strumenti informatici.

La Fondazione Luca Pacioli ha provveduto a proporre la questione all'Autorità Garante.
In attesa che il Garante fornisca chiarimenti in merito, propendiamo per un'interpretazione rigida della norma, ci sembra, cioè, che il DPS vada redatto in ogni caso si trattino dati personali con l'ausilio degli strumenti elettronici senza che rilevi la tipologia dei dati in questione se si tratti cioè di dati sensibili e giudiziari o meno. Questa considerazione consegue ad un duplice ordine di constatazioni: innanzitutto, da un esame attento delle informazioni contenute nel DPS (vedi qui sotto) non sembra possibile risalire ad una limitazione della compilazione del documento per i soli casi di dati sensibili e giudiziari, in secondo luogo si rileva che, proprio il codice, introduce all'art. 1 il diritto alla tutela dei dati personali (v. paragrafo 1) in genere.

Il DPS deve essere redatto entro il 31 marzo di ogni anno e riportare le seguenti informazioni:

- 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, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed 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, 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, nonchè in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento dei dati personali;
- 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;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione dagli altri dati personali dell'interessato.

Da ultimo si segnala il punto 26 dell'allegato b) del Codice : "Il titolare riferisce, nella relazione accompagnatoria del bilancio di esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico".

4. Sanzioni

Se non vengono rispettate le misure di adeguamento al T.U. si rischiano sanzioni molto severe. Sono previste multe dai 3.000 ai 50.000 € e la reclusione fino a 3 anni. Qui di seguito è riportata una tabella delle sanzioni relative alle diverse tipologie di illecito.

ILLECITI CIVILI	**SANZIONE**
Art. 161 Omessa o inidonea informativa	Sanzione da 3.000 € a 18.000 €
Art. 161 Omessa informativa per dati sensibili o giudiziari o in caso di trattamenti che presentano rischi specifici o di maggiore rilevanza o di pregiudizio	Sanzione da 5.000 € a 30.000 €
Art. 163 Omessa o incompleta notificazione al Garante	Sanzione da 10.000 € a 60.000 €
Art. 164 Omessa informazione o esibizione dei documenti richiesti dal Garante	Sanzione da 4.000 € a 24.000 €
ILLECITI PENALI	**SANZIONE**
Art. 167 Trattamento illecito di dati personali	Reclusione da 6 mesi a 3 anni. Possibile estinguere il reato ex art. 169, pagando una somma di denaro se ci si regolarizza entro il termine prescritto (non + di 6 mesi)
Art. 168 Falsità nelle dichiarazioni e notificazioni al Garante	Reclusione da 6 mesi a 3 anni
Art. 169 Omessa adozione delle misure minime di sicurezza	Arresto fino a 2 anni o sanzione amministrativa, pagamento di una somma da 10.000 € a 50.000 €
Art. 170 Innosservanza dei provvedimenti del Garante	Reclusione da tre mesi a due anni

5. Termini stabiliti per l'adeguamento alle nuove disposizioni

Termine ultimo per adeguarsi alle nuove disposizioni del Testo Unico era il 1° gennaio 2004, data di entrata in vigore del codice (art. 186).
L'art. 180 delle disposizioni transitorie del T.U., però, stabilisce che le nuove misure minime di sicurezza, non previste dalla precedente normativa, possano essere adottate entro il 30 giugno 2004.

Tra le misure di sicurezza da attuare entro il termine del 30 giugno 2004 non pare, però, possa farsi rientrare la compilazione del Documento Programmatico sulla Sicurezza in quanto tale documento era già previsto dalla precedente normativa (art. 6 del DPR 28.7.99 – n. 318). Pertanto il DPS dovrà essere redatto entro il 31 marzo 2004. Si potrebbe però obiettare che, nel caso in cui il documento sia obbligatorio per coloro che trattino dati personali di qualunque genere con l'ausilio di strumenti elettronici (come da noi sostenuto), l'ambito di applicazione soggettivo della norma non coincida più con la precedente disposizione di legge. Si ricorda che l'art. 6 del DPR 28.7.99 prevedeva la redazione di tale documento solo per il trattamento di dati sensibili e giudiziari. Si può allora ipotizzare che per coloro che non avevano, stando alla precedente normativa, l'obbligo di redazione del DPS, lo stesso possa configurarsi come "nuova misura di sicurezza" la cui adozione, pertanto, risulterebbe rinviata al 30 giugno 2004. Inoltre, essendo espressamente stabilito il termine del 31 marzo (allegato b), punto 19) potrebbe aversi una scadenza per la prima compilazione del DPS al 31 marzo 2005. Come è evidente la questione è controversa. Anche questo aspetto, pertanto, è stato posto dalla Fondazione Luca Pacioli all'attenzione del Garante.

Un'ultima importante segnalazione riguarda la possibilità di richiedere una proroga ex art. 180, T.U. privacy, per l'adeguamento degli strumenti informatici alle misure minime di sicurezza al 1° gennaio 2005. La proroga può essere richiesta esclusivamente da parte dei titolari di trattamento che, alla data di entrata in vigore del codice, disponevano di strumenti elettronici che, per obiettive ragioni tecniche, non consentivano in tutto o in parte l'immediata applicazione delle misure minime di sicurezza. Chi fosse interessato alla richiesta di proroga al 1.1.2005, dovrà elencare le motivazioni della richiesta in un apposito documento a data certa da conservare presso la propria struttura.

6. Schema riassuntivo degli adempimenti da adottare in materia di privacy

1) Identificazione del titolare del trattamento
2) Notifica al Garante dell'inizio del trattamento (solo ove richiesta)
3) Richiesta dell'Autorizzazione ad effettuare il trattamento dei dati (solo ove richiesta)

4) Nomina dei soggetti coinvolti nel trattamento:
   - Responsabile / i del trattamento (facoltativo)
   - Incaricato / i al trattamento
5) Predisposizione misure di sicurezza per trattamenti effettuati senza strumenti informatici:
   - 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.
6) Predisposizione misure minime di sicurezza per trattamenti effettuati con strumenti informatici:
   - autenticazione informatica;
   - credenziali di autenticazione;
   - sistema di autorizzazione;
   - aggiornamento periodico;
   - protezione degli strumenti elettronici e dati;
   - procedure per la custodia di copie di sicurezza;
   - redazione del DPS;
   - adozione di tecniche di cifratura o di codici identificativi per trattamento dati idonei a rivelare stato di salute o vita sessuale.
7) Informazione all'interessato in merito al trattamento dei suoi dati (salvo eccezioni)
8) Acquisizione del consenso, scritto ed informato, dell'interessato (salvo eccezioni)

APPENDICE

Glossario dei termini utilizzati dal legislatore

L'art. 4 del testo unico in materia di privacy raggruppa in un'unica disposizione le definizioni dei termini specifici della disciplina. Per agevolare la comprensione della presente circolare e del testo di legge, si specifica, qui di seguito, il significato di alcuni termini utilizzati dal legislatore:

"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;

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

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

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

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

"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;

"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;

"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;

"dati giudiziari", i dati personali idonei a rive lare 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;

“dati identificativi”, i dati personali che permettono l’identificazione diretta dell’interessato;

“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;

“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 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;

“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;

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

“Garante”, l’autorità di cui all’articolo 153, istituita dalla legge 31 dicembre 1996, n. 675;

“incaricati”, le persone fisiche autorizzate 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;

“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;

“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;

“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;

“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;

“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;

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

“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;

“scopi storici”, le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

“scopi statistici”, le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

“scopi scientifici”, le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore;

“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;

“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;

“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;

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

“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;

“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;

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

FONDAZIONE LUCA PACIOLI