CIRCOLARE N.4/2006

Protezione dei dati personali

Premessa

Si porta a conoscenza che in data 30 giugno 2003 il Consiglio dei Ministri ha approvato il Decreto Legislativo, n.196 pubblicato in Gazzetta Ufficiale n.174 del 29 luglio 2003 con il quale è stato istituito il nuovo "Codice in materia di protezione dei dati personali" (di seguito denominato Codice).

Il Codice, ispirato all'introduzione di maggiori garanzie nel trattamento dei dati personali ed alla semplificazione delle norme esistenti, riunisce in unico testo normativo la legge n. 675/1996, tutti i decreti e provvedimenti ad essa collegati e, anche alla luce delle pronunce e dei pareri forniti in questi anni dal Garante della privacy, può essere considerato un testo unico in materia.

L'entrata in vigore del presente decreto è stata inizialmente fissata, dall'art.180 dello stesso decreto, al 30 giugno 2004 ma ha subito diverse proroghe:

- il decreto legge 24 giugno 2004 n.158, pubblicato in Gazzetta Ufficiale n. 147 del 25 giugno 2004, ha sancito la proroga al 31 dicembre 2004;
- il decreto legge 9 novembre 2004 n.266, pubblicato in Gazzetta Ufficiale n. 264 del 10 novembre 2004 ha sancito la proroga al 30 giugno 2005;
- la legge 1° marzo 2005 n.26, che ha convertito in legge, con modificazioni, il decreto legge 30 dicembre 2004, n. 314, ha sancito la proroga al 31 dicembre 2005;
- il decreto-legge 30 dicembre 2005, n. 273, pubblicato in Gazzetta Ufficiale n. 303 del 30 dicembre 2005, ha prorogato il termine ultimo al 31 marzo 2006.

Pertanto entro il 31 marzo 2006 dovranno essere adottate le disposizioni previste dal Codice.

Impianto normativo

Il codice è diviso in tre parti:

- la prima è dedicata alle disposizioni generali necessarie per tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato;
- la seconda è dedicata alle disposizioni previste per settori specifici;

- la terza affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

Con il presente lavoro si intende fornire alcune indicazione in merito agli adempimenti da espletare per garantire il rispetto dei dati personali.
Ovviamente, tale lavoro non ha l'obiettivo di essere esaustivo, ma solo di fornire una informazione preliminare sull'applicazione della disposizione.

Analisi del provvedimento

Si sottolinea che la maggior parte delle difficoltà interpretative del Codice deriva dal fatto che la normativa individua i soggetti obbligati a determinati adempimenti, con riferimento generico alla tipologia ed alla modalità di trattamento dati.
Ciò significa che non è possibile fornire indicazioni valide per tutte le aziende o per tutti i professionisti, in quanto ogni soggetto potrebbe utilizzare tipologie di dati differenti rispetto ad un altro.
Il primo passo da compiere, dunque, è quello dell'identificazione dei dati soggetti a trattamento e delle modalità con cui tali dati sono trattati (con o senza l'ausilio di strumenti informatici).

Soggetti interessati

Il principio ispiratore del Codice risiede nel fatto che chiunque ha diritto alla protezione dei dati personali e il trattamento degli stessi debba essere svolto nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza e all'identità personale.
Il legislatore per trattamento ha inteso "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".
Dall'ampiezza della definizione appare chiaro che la normativa in oggetto interessa un ampio raggio:
- di trattamenti: qualunque operazione concernente dati personali effettuata con o senza l'ausilio di strumenti elettronici;

- di soggetti: qualunque soggetto, pubblico o privato, che effettui il trattamento di dati personali, sia esso una società, un'impresa, uno studio professionale o una pubblica amministrazione.

Nessuno è esente dalla disciplina ad eccezione delle persone fisiche che effettuano il trattamento per fini esclusivamente personali, a condizione che i dati non vengano destinati ad una comunicazione sistematica o alla diffusione, e purché il trattamento venga effettuato nel rispetto dell'obbligo di adottare quelle misure di sicurezza finalizzate a ridurre al minimo i rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito, o comunque non conforme alle finalità della raccolta.

Soggetti che effettuano il trattamento dei dati

Sono coinvolte tutte le persone che svolgono operazioni inerenti i dati personali all'interno di una struttura aziendale o di uno studio professionale, dove occorre necessariamente distinguere tra titolare, responsabile e incaricato del trattamento:

- titolare del trattamento è il soggetto che esercita un potere decisionale autonomo in merito alle finalità e alle modalità del trattamento, compreso naturalmente il profilo della sicurezza.

  Può essere una persona fisica o giuridica, ovvero qualsiasi soggetto inteso come centro di interessi giuridici e patrimoniali quale entità nel suo complesso. Ad esempio, in un'azienda che effettua il trattamento di dati, il titolare non è colui che rappresenta l'azienda, ma l'azienda in senso lato, mentre il rinvio alla persona fisica va riferito ai soggetti privati, professionista o imprenditore persona fisica;
- responsabile del trattamento è colui che è scelto dal titolare perché possiede caratteristiche che per esperienza, capacità ed affidabilità, sono idonee a fornire la garanzia del pieno rispetto delle disposizioni in materia di trattamento.

  Questi deve attenersi alle istruzioni del titolare, il quale ha l'obbligo di verificare periodicamente l'operato del responsabile e conserva una responsabilità per culpa in eligendo ed in vigilando;
- incaricato è il soggetto, necessariamente una persona fisica, che esercita operazioni di trattamento sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

Il titolare del trattamento dei dati personali deve specificare per iscritto i compiti affidati responsabile e, per quanto riguarda gli incaricati, la designazione deve essere effettuata per iscritto e deve individuare precisamente l'ambito del trattamento consentito.

Nessun trattamento può essere operato da soggetti diversi dal titolare, responsabile o incaricato.

Modalità di trattamento dei dati

Le modalità di trattamento dati, sanciti dall' art. 11 del Codice, stabilisce che i dati personali oggetto di trattamento debbano 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.

Principali adempimenti

Il quadro degli obblighi per i soggetti interessati si ricostruisce andando a consultare diverse norme disposte in ordine sparso nel Codice; non è sufficiente consultare il Titolo VI della parte I, specificamente rubricato "Adempimenti", dato che lo stesso riguarda solo la notificazione del trattamento e gli obblighi di comunicazione e di autorizzazione.

I principali adempimenti da adottare possono essere così individuati:

1. gli interessati o le persone presso le quali sono raccolti i dati devono ricevere una specifica informativa;
2. il trattamento di dati personali da parte di privati o di enti pubblici economici richiede l'acquisizione del consenso da parte dell'interessato;
3. il trattamento di dati sensibili deve avvenire in conformità con quanto previsto dall'art.37 del Codice;
4. le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) del Codice devono essere adottate entro il 31 marzo 2006, sia per i dati trattati con strumenti che per quelli trattati con strumenti elettronici;

5. documento programmatico sulla sicurezza.

1.Informativa sulla "privacy"

L'art. 13 del Codice sancisce l'obbligo di informativa nei confronti dell'interessato in riferimento alle finalità e alle modalità del trattamento dati, alla natura obbligatoria o facoltativa del conferimento dati, alle conseguenze di un eventuale rifiuto a fornire dati, all'eventuale comunicazione dei dati ai terzi ed il loro ambito di diffusione.

L'interessato deve, altresì, 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.

L'informativa può essere resa per iscritto o anche, in forma orale.

Di seguito si allega una bozza della lettera informativa.

INIZIO"

Agli interessati
Loro sedi

Informativa sul trattamento dei dati personali ai sensi dell'art. 13 del D.lgs n. 196/03 "Codice per la protezione dei dati personali"

Egregi Signori,
il decreto Legislativo n. 196/03 "**Codice per la protezione dei dati personali**" (nel seguito il "CODICE") ha dettato una disciplina uniforme in materia di tutela dei dati personali delle persone giuridiche e fisiche.

XY S.r.l. (nel seguito XY), in virtù del rapporto contrattuale con Voi in corso, raccoglie e tratta dati personali relativi alla Vostra Società/persona.

Pertanto, in considerazione dell'obbligo di informativa nei confronti dei soggetti interessati cui i dati personali si riferiscono, ai sensi dell'art. 13 del CODICE, si riporta qui di seguito l'informativa di cui in oggetto,

a) <u>TITOLARE DEL TRATTAMENTO E GESTORE DEI DATI</u>

Titolare del trattamento dei Vostri dati personali è **XY S.r.l.** con sede in ……, Via …… CAP ……..nella persona del Sig……..
Il Titolare, pertanto è tenuto a fornire un'esauriente informativa in relazione alla raccolta e all'utilizzo dei dati personali e deve garantire che il trattamento si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché nella dignità delle persone fisiche, con particolare riguardo

alla riservatezza e all'identità personale, in modo che l'interessato possa manifestare consapevolmente, ove necessario, il proprio consenso "informato".

b) FONTE DEI DATI PERSONALI

I dati personali in nostro possesso sono raccolti direttamente presso di Voi in occasione della stipula del contratto o in costanza di rapporto.

c) FINALITA' DEL TRATTAMENTO

Il trattamento dei dati personali è effettuato esclusivamente per finalità strettamente necessarie e connesse alla gestione dei rapporti contrattuali con voi in corso e comunque per l'adempimento degli obblighi previsti dalla legge, da regolamenti, da disposizioni impartite da autorità o da organismi di vigilanza a ciò legittimati, al fine della corretta conduzione ed esecuzione del rapporto ed in ogni caso in maniera non eccedente rispetto alle finalità indicate.

d) DATI OGGETTO DEL TRATTAMENTO

In relazione alle finalità indicate, oggetto di trattamento sono i dati anagrafici della Vostra Società tra cui a titolo esemplificativo: nome, cognome, data e luogo di nascita, codice fiscale, partita iva, numeri di telefono, coordinate bancarie e, comunque, ogni altro dato identificativo utile per la gestione del rapporto contrattuale.

e) MODALITA' DEL TRATTAMENTO

Il trattamento dei Vostri dati personali viene effettuato dalla XY S.r.l. che si avvale della propria struttura a ciò deputata.
Le operazioni di trattamento avvengono mediante strumenti informatici e cartacei comunque con logiche strettamente connesse alle suddette finalità in modo da garantire la sicurezza e la riservatezza dei dati.
A tal fine accederanno al trattamento soltanto i soggetti a ciò autorizzati.
In particolare ai sensi dell'art. 11 del CODICE i dati:

- vengono trattati in modo lecito e secondo correttezza;
- vengono raccolti e registrati per gli scopi indicati ed eventualmente utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- sono esatti e se necessario, aggiornati;
- sono pertinenti, completi e non eccedenti alle finalità per le quali sono raccolti e successivamente trattati;
- vengono 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 sono stati raccolti o successivamente trattati;
- i dati che a seguito di verifiche risulteranno eccedenti o non pertinenti non verranno utilizzati, salvo che per l'eventuale conservazione a norma di legge del documento che li contiene.

f) NATURA DEL CONFERIMENTO DEI DATI ED EVENTUALI CONSEGUENZE DEL RIFIUTO DI RISPONDERE

In considerazione delle finalità di trattamento, il conferimento dei dati ha natura obbligatoria e non facoltativa. Pertanto l'eventuale rifiuto da parte Vostra di fornire le informazioni richieste potrebbe comportare l'impossibilità di adempiere correttamente alle suddette finalità, nonché all'impossibilità di proseguire il rapporto contrattuale con Voi in corso.

g) COMUNICAZIONE E DIFFUSIONE DEI DATI

I suoi dati personali verranno comunicati ai dipendenti e/o collaboratori di XY S.r.l., esclusivamente per le finalità sopra indicate, nonché – oltre ai soggetti ai quali la comunicazione è dovuta per legge – anche a soggetti terzi purché per finalità ed attività strettamente connesse alla gestione del rapporto contrattuale.

h) DIRITTI DELL'INTERESSATO

In ogni momento potrà esercitare i suoi diritti ai sensi dell'art. 7 del D.lgs. 196/2003 con richiesta rivolta, senza formalità, a XY S.r.l., Via……..– CAP Città…… - , al seguente numero di fax …….
Per Vostra comodità riportiamo qui di seguito il testo integrale dell'art. 7 del CODICE.

"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 si 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 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."

XY S.r.l.
L'Amministratore Unico
(……)

_____
Timbro e firma dell'interessato

FINE"

2.Consenso da parte dell'interessato

Successivamente alle informazioni ricevute sui propri diritti, affinché i dati possano essere trattati lecitamente, è necessario che l'interessato fornisca il consenso al trattamento dei dati personali ai sensi dell'art. 23 del Codice.

In deroga a tale regola di generale applicazione, l'art. 24 del Codice prevede alcune ipotesi in cui il trattamento dei dati personali può essere effettuato senza che sia necessario raccogliere il consenso.

Tra queste, si segnala che la raccolta del consenso non debba essere effettuata quando:

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

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;
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 del Codice;
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.

Per rendere più rapida la conclusione del procedimento si consiglia di inserire la dichiarazione di consenso nella parte terminale della bozza proposta al punto precedente apponendo tale dicitura:

“Il sottoscritto/la scrivente Società dichiara di aver ricevuto e compreso la presente informativa ai sensi dell’art. 13 D.lgs 196/2003 ed esprime/non esprime il proprio consenso al trattamento e correlate comunicazioni dei propri dati per le finalità precisate”.

3.Trattamento dei dati personali sensibili e notifica al Garante

Per dato personale si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati.

E' da considerarsi dato personale anche quello relativo a uno dei soggetti indicati non identificato (ad esempio, senza indicazione del nome e cognome), ma tuttavia identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Nell'ambito della amplissima categoria dei dati personali (qualunque informazione), vanno distinte alcune informazioni che, per la loro delicatezza, ricevono una particolare tutela: i dati sensibili e quelli giudiziari.

Per dati sensibili, si intendono 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.

Per dati giudiziari si intendono i dati personali idonei a rivelare i provvedimenti iscritti nel casellario giudiziale, nonché i dati idonei a rivelare la qualità di imputato ed indagato.

L’art. 37 del Codice identifica i casi in cui deve essere effettuata la notificazione al Garante, limitando l’obbligo di notificazione esclusivamente per quelle tipologie di dati che per loro natura rivestono una particolare delicatezza.

Pertanto devono essere notificati i trattamenti di dati:

- genetici, biometrici o di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica, ad eccezione dei trattamenti non sistematici di dati genetici o biometrici effettuati da esercenti le professioni sanitarie;

- idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria, con esclusione di quelli effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti;
- 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;
- trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica, con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- dati 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.

La notificazione al Garante deve essere effettuata prima dell'inizio del trattamento dei dati personali.

La notifica è unica, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.

4.Misure minime di sicurezza

La normativa riporta una serie di indicazioni generali riguardo agli interventi minimi da realizzare, descritti in dettaglio all'interno dell'allegato B - "Disciplinare tecnico in materia di misure minime di sicurezza"

I responsabili, nel caso di trattamenti con l'ausilio di strumenti elettronici hanno alcuni obblighi in quanto devono:

- disporre di credenziali di autenticazione (es. password) individuali che devono essere ideate, gestite ed aggiornate secondo criteri di sicurezza, e quindi ad esempio non devono corrispondere alla propria data di nascita e devono essere modificate almeno ogni 6 mesi (3 in caso di dati sensibili o giudiziari).

- definire i profili di autorizzazione degli incaricati, che definiscono a quali dati l'incaricato può accedere, nonché i trattamenti a lui consentiti e devono essere individuati in modo tale da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento; gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggere i difetti devono essere effettuati con cadenza almeno annuale.
- assicurarsi che i dati personali devono essere protetti da trattamenti illeciti e da accessi non consentiti anche mediante l'attivazione di idonei programmi (es. antivirus, firewall,) che devono essere correttamente installati e settati ed aggiornati con cadenza almeno semestrale.
- essere impartite istruzioni organizzative e tecniche che prevedono:

    - il salvataggio dei dati con frequenza almeno settimanale;
    - l' adozione di procedure per la custodia delle copie di sicurezza,
    - le modalità di ripristino della disponibilità dei dati e dei sistemi in caso di danneggiamento.

Per i casi in cui la limitatezza tecnologica degli strumenti in uso o la loro obsolescenza non consentano di attuare completamente il dettato normativo, si prevede l'obbligo da parte del titolare di descrivere in un documento a data certa, da custodire presso la propria struttura, gli impedimenti tecnici che hanno reso impossibile o parziale l'immediata applicazione delle misure minime di sicurezza per poter godere del termine di ulteriori tre mesi per adeguare la propria dotazione tecnologica in modo da consentire l'applicazione delle misure minime di sicurezza.

Per i trattamenti senza l'ausilio di strumenti elettronici, i responsabili devono prevedere:

- procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati;
- 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.

5.Documento programmatico sulla sicurezza

Tra le misure minime di sicurezza previste per il trattamento dati sensibili e giudiziari con l'ausilio di strumenti informatici rientra la redazione di un documento programmatico sulla sicurezza (DPS).

Il DPS deve contenere, principalmente, le informazioni relative ai dati trattati ed alle modalità di trattamento, l'analisi dei rischi che incombono sui dati e le misure adottate per evitarne la dispersione o la distruzione anche accidentale.

L'obbligo di redazione del documento programmatico sulla sicurezza ricorre in caso di trattamento di dati personali sensibili o giudiziari con strumenti elettronici (es. computer).

Pertanto, il documento programmatico sulla sicurezza non trova applicazione qualora si proceda unicamente al trattamento di dati personali diversi da quelli sensibili o giudiziari, anche se effettuati con strumenti elettronici.

Il Documento deve contenere idonee informazioni in primo luogo riguardo:

- l'elenco dei trattamenti effettuati;
- la distribuzione di compiti e responsabilità;
- l'analisi dei rischi che incombono sui dati;
- le misure di sicurezza adottate e da adottare;
- i criteri di ripristino dei dati a seguito di distruzione o danneggiamento;
- la formazione degli incaricati;

Misure ulteriori sono previste a protezione dei dati sensibili o giudiziari nel caso di trattamenti effettuati senza l'ausilio di strumenti elettronici:

- devono essere impartite istruzioni scritte agli incaricati finalizzate al controllo e alla custodia degli atti e dei documenti contenenti dati personali.
- deve essere previsto l'aggiornamento almeno annuale dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati.
- l'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato.

In riferimento alle modalità di formazione e compilazione del DPS è stato predisposto dal Garante della privacy una guida operativa pertanto si rinvia alla stessa per una analisi dettagliata (versione scaricabile da www.garanteprivacy.it).

In attesa di chiarimenti, non risulta agevole definire se, per la categoria degli operatori economico-contabili, sia obbligatoria la redazione del DPS.
Dall'analisi dei dati oggetto di trattamento da parte dei commercialisti non sembrerebbe ravvisarsi il trattamento di dati sensibili e/o giudiziari con l'ausilio di strumenti informatici.
I maggiori dubbi nascono in riferimento ai dati relativi alle spese mediche e alla destinazione dell'otto per mille trattati all'interno della dichiarazione dei redditi (trasmessa per via telematica):
In merito alle spese mediche si ritiene che non possano essere ritenute dato sensibile in quanto non riconducibili alla patologia del contribuente, ma semplicemente e genericamente ad un importo versato.
Per quanto attiene all'analisi della destinazione dell'otto per mille si ritiene gli stessi non possano essere considerati dati sensibili in quanto nella fattispecie si ravvisa una destinazione di risorse allo Stato e non una confessione religiosa dalla cui destinazione possa ricondursi, una manifestazione di convinzione religiosa.

Privacy e bilancio

La nuova disciplina sul trattamento dei dati personali ha riflessi anche sulla redazione dei bilanci.
Infatti, il punto 26 dell'allegato B del Codice dispone che "il titolare riferisce, nella relazione accompagnatoria del bilancio di esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza".
Pertanto nella relazione accompagnatoria al bilancio di esercizio deve darsi notizia dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.
Tuttavia, poiché la norma prende in considerazione la relazione accompagnatoria del bilancio d'esercizio "se dovuta", si ritiene che le società che redigono il bilancio abbreviato e che sono esonerate dal predisporre la relazione sulla gestione, ai sensi dell'art. 2435-bis c.c., siano conseguentemente escluse anche dall'adempimento in esame.

Sanzioni

Il primo comma dell'art. 169 del Codice dispone che chiunque, essendovi tenuto, omette di adottare le misure minime di sicurezza previste dall'art. 33, tra cui il documento programmatico

sulla sicurezza, è soggetto alla sanzione penale dell'arresto fino a due anni o dell'ammenda da 10.000,00 a 50.000,00 euro.

Il secondo comma prevede però una sorta di "ravvedimento operoso" basato:

- sulla regolarizzazione entro un determinato termine, comunque non superiore a 6 mesi;
- sul pagamento di una sanzione ridotta, pari al quarto del massimo dell'ammenda (quindi 12.500,00 euro).

Si resta a disposizione per ogni eventuale chiarimento

Napoli, 17 marzo 2006

Dott. Maurizio Moccaldi Ruggiero