Fondazione Luca Pacioli

LA DISCIPLINA SULLA PRIVACY

Aggiornamento sugli adempimenti

Documento n. 13 del 6 maggio 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

LA DISCIPLINA SULLA PRIVACY

Aggiornamento sugli adempimenti

Introduzione

Il Codice in materia di protezione dei dati personali (introdotto con D.Lgs. 30 giugno 2003, n. 196) è legge vigente dal 1° gennaio 2004. A più di quattro mesi dalla sua entrata in vigore, tenuto conto dei numerosi quesiti pervenuti sulla materia, sembra opportuno ritornare sull'argomento (la Fondazione Luca Pacioli ha già pubblicato due circolari in merito[1]) per chiarire taluni aspetti di incerta interpretazione. Per migliore chiarezza, si è ritenuto di riproporre il testo di tali precedenti circolari, con le necessarie integrazioni e specificazioni.

L'illustrazione della disciplina – oggettivamente complessa e per questo riferita nelle sue linee essenziali per semplificare la esposizione - riguarda gli adempimenti che fanno carico a tutti i soggetti che *trattano dati personali* e che sono pertanto obbligati ad attenersi alle disposizioni del Codice Privacy.

Le informazioni fornite possono pertanto rappresentare un utile supporto anche per l'individuazione degli adempimenti posti a carico dei professionisti dell'area economico-contabile, in relazione ai dati personali da loro trattati per l'esercizio dell'attività professionale. In questo senso, si è provveduto, a conclusione di ciascun paragrafo, a specificare se la materia trattata possa essere di interesse o meno per i professionisti dell'area economico-contabile e per i Collegi provinciali (si veda pure la tabella di sintesi degli adempimenti, paragrafo 8).
Si anticipa subito che i professionisti ed i Collegi sono interessati a tutti gli adempimenti di seguito illustrati con eccezione degli adempimenti nei confronti dell'Autorità Garante (vedi paragrafo 5).

Naturalmente le indicazioni fornite tengono conto del **trattamento dei dati correlato alla normale attività professionale**. Va da sé che tali indicazioni andranno opportunamente verificate ed integrate qualora la raccolta dei dati personali fosse riferita ad attività straordinarie rispetto alla normale operatività.

I contenuti della circolare possono fornire inoltre le informazioni di base circa la disciplina Privacy applicabile alla generalità dei soggetti che trattano dati personali. I professionisti contabili possono pertanto ricavarne le indicazioni essenziali per

1 Circolare "Codice della Privacy – Testo unico in materia di protezione dei dati personali", Documento n. 9 del 19 marzo 2004, Circolare "Codice della Privacy – Documento Programmatico sulla Sicurezza" Documento n. 10 del 31 marzo 2004.

orientarsi circa gli adempimenti dalla loro clientela, fermo rimanendo che sarà indispensabile effettuare un'analisi delle singole fattispecie, sulla base delle caratteristiche del trattamento dei dati personali di volta in volta realizzato.
A questo proposito, si sottolinea infatti che le maggiori difficoltà interpretative derivano dalla circostanza che le norme, nello stabilire gli adempimenti dovuti, non fanno riferimento ai soggetti distinti per categorie o per l'attività svolta, bensì ai soggetti individuati sulla base della tipologia e delle modalità di trattamento dati (si veda il paragrafo 1). Ciò significa che non è possibile fornire indicazioni valide per tutte le aziende o per tutti i professionisti, né è possibile fornire indicazioni per singole categorie di aziende o di professionisti, in quanto ogni soggetto che tratti dati personali è tenuto ad osservare la specifica disciplina riferita alla tipologia di dati trattati ed ai differenti modi di trattazione dei dati stessi.

Dunque, il primo passo da compiere per orientarsi è quello di identificare la tipologia dei dati soggetti a trattamento (*dati personali, dati sensibili, dati giudiziari*. Vedi paragrafo 1).
I dati personali infatti sono tutti soggetti a tutela ma per la categoria più limitata dei *dati sensibili* e *giudiziari* sono previsti adempimenti e misure di sicurezza particolarmente rigorosi.
Altra distinzione fondamentale riguarda la modalità con la quale i dati personali sono trattati: dati trattati con l'ausilio di strumenti informatici (*computer*) o senza (i c.d. trattamenti "cartacei", pratiche, faldoni, fascicoli, ecc.).

1. Principali termini utilizzati dal legislatore

E' indispensabile, ai fini della chiarezza espositiva, riportare in apertura i principali termini utilizzati dal legislatore.

Per **trattamento** si intende 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 personali*, anche se non registrati in una banca dati. In sostanza, la raccolta e la conservazione *di dati personali* assumono sempre rilievo, sia se effettuate su carta, sia se effettuate mediante *computer*.

Per **dato personale** si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati. E' 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[2]: in altre parole, si tratta dei dati relativi agli eventuali procedimenti penali a carico della persona.

2. Soggetti obbligati e sintesi degli obblighi previsti

Sono tenuti ad osservare le disposizioni sulla privacy tutti coloro che *trattano* dati personali, vale a dire:
- Aziende
- Pubbliche Amministrazioni
- Professionisti

Quello che rileva è il trattamento dei dati personali. In altri termini, il soggetto (azienda, pubblica amministrazione, professionista) che per qualsiasi motivo raccoglie dati personali è obbligato a rispettare le norme sulla privacy.

La disciplina di tutela dei dati personali, ora contenuta nel cosiddetto Codice Privacy, prevede una serie di obblighi.
Si possono distinguere in proposito:

1) L'individuazione dei soggetti che effettuano il trattamento dei dati personali (con la distinzione delle figure del *titolare*, del *responsabile*, del / degli *incaricato/i*);
2) Le regole generali da osservare per il trattamento dei dati personali, vale a dire gli adempimenti che debbono essere osservati in ogni caso nei confronti dei soggetti i cui dati personali vogliano essere trattati:

a) *modalità del trattamento e requisiti dei dati;*
b) *informativa;*
c) raccolta del *consenso*;

2 Con ciò innovando notevolmente la precedente formulazione, che riguardava solo i provvedimenti iscritti nel casellario giudiziale.

3) Gli adempimenti nei confronti dell'Autorità Garante nel caso di trattamento di dati personali sensibili e giudiziari:
   a) la *notificazione* del trattamento dei dati;
   b) la *comunicazione* di particolari circostanze all'Autorità Garante;
   c) la richiesta di *autorizzazione;*
   4) le *misure di sicurezza* da adottare per la tutela dei dati personali raccolti (*misure idonee* e *misure minime*).

I professionisti dell'area economico-contabile ed i Collegi provinciali, non sono soggetti a nessuno degli adempimenti previsti nei confronti dell'Autorità Garante di cui al precedente punto 3 (notificazione, comunicazione e richiesta di autorizzazione), (semprechè i dati trattati non esulino dalla loro normale attività).

3. Soggetti che effettuano il trattamento dei dati personali

La raccolta e la conservazione dei dati personali (trattamento dei dati) può coinvolgere, oltre al soggetto obbligato per legge, anche altri soggetti che, in ausilio del soggetto obbligato, collaborano agli adempimenti relativi. La legge distingue in proposito le seguenti figure:

Il titolare del trattamento
che è 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 ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Nel caso dei professionisti, *titolare del trattamento* è considerato il libero professionista che esercita la professione individualmente. Se l'attività professionale venga esercitata in forma associata, *titolare del trattamento* risulterà l'associazione nel suo complesso. Nel caso dei Collegi provinciali titolare del trattamento è il collegio stesso.

Accanto alla figura del *titolare del trattamento,* definita direttamente dalla legge, sono individuabili due altre figure solo eventuali, traendo esse origine da un atto di nomina facoltativo:

Il Responsabile del trattamento
che è la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal *titolare* al trattamento dei dati personali.
La designazione del responsabile è atto discrezionale ma, se compiuto, obbliga al rispetto di precisi criteri nella scelta del soggetto. Il responsabile, infatti, deve essere individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo della sicurezza.

I compiti affidati al responsabile devono essere *specificati per iscritto* dal titolare (art. 29, comma 4 del Codice).

Gli Incaricati del trattamento
che sono le persone fisiche autorizzate a compiere operazioni di trattamento dal *titolare* e dal *responsabile*. Si tratta di una figura subordinata rispetto al titolare e al responsabile, il cui incarico si limita allo svolgimento materiale delle operazioni relative al trattamento dati.
La designazione degli incaricati deve essere *effettuata per iscritto*, e deve indicare puntualmente l'ambito del trattamento consentito (art. 30, comma 2 del Codice).

I professionisti dell'area economico-contabile ed i Collegi provinciali, se ne sentiranno l'esigenza, potranno procedere alla designazione di uno o più responsabili e incaricati del trattamento. In tal caso dovranno essere osservate le formalità sopra specificate.

4. Regole generali per il trattamento dei dati personali

I soggetti che trattino dati personali, obbligati pertanto alla osservanza delle disposizione sulla privacy (aziende, pubbliche amministrazioni, professionisti), devono provvedere in ogni caso:

- a trattare i dati secondo le modalità ed i requisiti richiesti dalla legge;
- a dare una serie di informazioni (*informativa*) ai soggetti i cui dati si vogliano raccogliere;
- ad ottenere che i medesimi soggetti prestino il consenso alla raccolta dei dati personali.

4.1. Modalità del trattamento e requisiti dei dati

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*.

4.2. Informativa

Prima di poter trattare qualsiasi tipo di dato personale (sia esso solo personale o anche *sensibile* o *giudiziario*), è necessario dare talune informazioni (*informativa*) a coloro che forniscono i propri dati. Tra le novità del Codice Privacy è adesso consentito che l'*informativa* sia resa per iscritto o anche, in forma orale.

L'informazione resa deve riguardare:

- le finalità e le modalità del trattamento cui i dati sono destinati
- la natura obbligatoria o facoltativa del conferimento dei dati
- le conseguenze di un eventuale rifiuto a rispondere
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di *responsabili* o *incaricati*, e l'ambito di diffusione dei medesimi
- i diritti di cui all'art. 7[3] del Codice
- gli estremi identificativi del *titolare*[4] e, se designato, del *responsabile*[5].

L'omessa o inidonea informativa è punita con sanzione amministrativa dai 3.000 ai 18.000 € nel caso dei dati personali, e da 5.000 a 30.000 € per dati sensibili o giudiziari.

---

3 *Art. 7 (Diritto di accesso ai dati personali ed altri diritti)*

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4 L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, 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.
4 e se designato del rappresentante nel territorio dello Stato ai sensi dell'art. 5, nel caso di *titolare* non residente.

5 Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Nel caso in cui se ne senta l'esigenza, accanto al responsabile, può essere designato altro specifico responsabile al quale rivolgersi per l'esercizio dei diritti di cui all'art. 7. L'informativa deve dare indicazione anche di questo soggetto.

Si ricorda che, seguito delle modificazioni legislative intervenute, dal 1° gennaio 2004 l'informativa deve essere resa ai sensi dell'art. 13 del D.Lgs. 196/2003. Vanno conseguentemente modificati i riferimenti normativi da citare nelle comunicazioni da dare al soggetto interessato.

L'adempimento della informativa fa carico in ogni caso anche ai professionisti dell'area economico-contabile e ai Collegi provinciali.
Si è già detto che l'informativa può essere resa sia per iscritto che in forma orale. Tenuto conto tuttavia della complessità dell'informazione da dare, motivi di praticità e di cautela inducono a consigliare il rilascio dell'informativa in forma scritta (attraverso la predisposizione di un modello da conservare previa acquisizione della firma dell'interessato).

4.3. Consenso

In aggiunta all'informativa, è necessario che i soggetti i cui dati personali (anche se sensibili e giudiziari) si vogliano raccogliere prestino il proprio consenso alla raccolta dei loro dati personali.

In deroga a tale regola di generale applicazione, l'art. 24 del D.Lgs. 196/2003 prevede alcune ipotesi in cui il trattamento dei dati personali può essere effettuato senza che sia necessario raccogliere il consenso. Tra queste, si segnalano qui di seguito quelle principali:

- i casi previsti nella II parte del testo unico (disposizioni relative a specifici settori: trattamenti in ambito giudiziario, da parte di forze di polizia, per la difesa e sicurezza dello Stato, trattamenti in ambito pubblico, in ambito sanitario, riguardanti l'istruzione in ambito scolastico, per scopi storici, statistici o scientifici, riguardanti lavoro e previdenza sociale, il sistema bancario, finanziario ed assicurativo, effettuati da coloro che gestiscono servizi di comunicazione elettronica, trattamenti effettuati con finalità giornalistiche e di marketing diretto);
- quando il trattamento dei dati personali 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.

Al di fuori dei casi menzionati, il consenso dell'interessato al trattamento dei dati è sempre obbligatorio.

Alla luce di quanto riferito, preso atto che la raccolta del consenso non è necessaria "*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*", e tenuto conto che il rapporto professionale ha natura contrattuale, si ritiene che nella generalità dei casi i professionisti dell'area economico-contabile non siano tenuti alla raccolta del consenso.

5. Gli adempimenti rispetto all'Autorità Garante

A tutela di particolari categorie di dati sensibili o giudiziari, il Garante richiede che il *titolare* del trattamento segnali particolari circostanze o chieda una previa autorizzazione.
Gli adempimenti riguardano:

- la notificazione;
- la comunicazione;
- la richiesta di autorizzazione.

5.1. La Notificazione all'Autorità Garante

In taluni casi, la raccolta dei dati personali, *sensibili* e *giudiziari* (vedi paragrafo 1), deve essere notificata all'Autorità Garante.

Con provvedimento del 31 marzo 2004 e i successivi chiarimenti del 23 aprile 2004, l'Autorità Garante ha ulteriormente ridotto i casi in cui è necessario provvedere alla notifica.
In sintesi, l'obbligo di notificazione sopravvive esclusivamente per quelle tipologie di dati (in realtà molto limitate) che per loro natura rivestono una particolare delicatezza.
Per ulteriori informazioni sul tema delle notificazioni, può farsi riferimento alla circolare della Fondazione Luca Pacioli, documento n. 9 del 19 marzo 2004[6].

I professionisti dell'area economico-contabile ed i Collegi non risultano compresi tra i soggetti tenuti all'adempimento.

6 Si informa inoltre che, con comunicazione del 29 aprile scorso, il Garante ha permesso che le notificazioni del trattamento dati, iniziate e sospese fino a tale data, siano considerate validamente effettuate anche se completate ed inviate entro le ore 24.00 del 15 maggio. Ulteriori informazioni sul sito www.garanteprivacy.it.

5.2. Gli obblighi di comunicazione

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

1. comunicazioni di dati non autorizzati da specifiche disposizioni di legge o di regolamento tra soggetti pubblici;
2. il trattamento di dati idonei a rilevare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria[7].

I professionisti dell'area economico-contabile ed i Collegi non sono tenuti all'adempimento.

5.3. L'autorizzazione al trattamento dei dati sensibili o dei dati giudiziari

I dati personali *sensibili* e/o *giudiziari* (vedi paragrafo 1) possono essere trattati solo previa Autorizzazione del Garante (artt. 26 e 27 del Codice).

Per alleggerire gli oneri che incombono su coloro che trattano dati sensibili e giudiziari, il Garante ha adottato una serie di autorizzazioni generali per particolari categorie di titolari o per specifici trattamenti di dati[8] (art. 40).
In particolare, con deliberazione del 24 giugno 2003 (pubblicata in G.U. n. 191 del 19 agosto 2003), sono state prorogate le 7 autorizzazioni generali[9] rilasciate dal Garante che avranno efficacia fino al 30 giugno 2004.

I professionisti dell'area economico-contabile sono interessati a talune di queste autorizzazioni generali:

---

7 Vedi art. 110, comma 1, primo periodo, del Codice Privacy.

8 Il Garante, nella Relazione al Parlamento 1997, ha così motivato il ricorso alle autorizzazioni generali "a) Le autorizzazioni per categorie o collettive permettono all'organo di garanzia di svolgere la propria azione di tutela con organicità, procedendo attraverso ampie aggregazioni di attività omogenee e rivolgendosi non più in maniera frammentaria e parcellizzata a singoli soggetti, ma ad intere categorie. La generalità dell'approccio valorizza lo strumento autorizzativo, che da provvedimento di disciplina di specifiche situazioni diviene una fonte di regolamentazione più ampia di interessi di rango quasi-normativo; b) tale metodo conferisce alla formula atorizzatoria la possibilità di individuazione di momenti unitari, che rendono agevole e snella la salvaguardia di principi inderogabili connessi ai dati sensibili; c) l'autorizzazione collettiva non soltanto si ispira ai principi di snellimento dell'azione amministrativa, ma comporta una notevole semplificazione degli adempimenti spettanti ai soggetti preposti al trattamento e incide positivamente sui loro profili economici, implicando un risparmio nei costi di gestione."

9 Le autorizzazioni generali, nello specifico, sono:
- autorizzazione n. 1/2002 al trattamento dei dati sensibili nei rapporti di lavoro;
- autorizzazione n. 2/2002 al trattamento dei dati idonei a rilevare lo stato di salute e la vita sessuale;
- autorizzazione n. 3/2002 al trattamento dei dati sensibili da parte di organismi di tipo associativo e delle fondazioni;
- autorizzazione n. 4/2002 al trattamento dei dati sensibili da parte di liberi professionisti;
- autorizzazione n. 5/2002 al trattamento dei dati sensibili da parte di diverse categorie di titolari;
- autorizzazione n. 6/2002 al trattamento dei dati sensibili da parte degli investigatori privati;
- autorizzazione n. 7/2002 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

- autorizzazione 1/2002 al trattamento dei dati sensibili nei rapporti di lavoro;
- autorizzazione 4/2002 al trattamento dati sensibili da parte dei liberi professionisti.

Pertanto, i professionisti dell'area economico-contabile che trattino dati rientranti nell'ambito di applicazione di una delle predette autorizzazioni generali, non sono tenuti a richiedere altra autorizzazione al Garante.

Discorso analogo vale per i Collegi provinciali i quali sono interessati alle seguenti autorizzazioni generali:
- autorizzazione 3/2002 al trattamento dei dati sensibili da parte di organismi di tipo associativo e delle fondazioni;
- autorizzazione 7/2002 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

Pertanto, anche i Collegi provinciali che trattino dati rientranti nell'ambito di applicazione di una delle predette autorizzazioni generali, non sono tenuti a richiedere altra autorizzazione al Garante.

Per ulteriori informazioni sul tema dell'autorizzazione, può farsi riferimento alla circolare della Fondazione Luca Pacioli, documento n. 9 del 19 marzo 2004.

I professionisti dell'area economico-contabile ed i Collegi provinciali non sono tenuti all'adempimento.

6. Le misure di sicurezza da adottare per la tutela dei dati personali

I soggetti che trattino dati personali, obbligati pertanto alla osservanza delle disposizioni sulla privacy (aziende, pubbliche amministrazioni, professionisti), devono provvedere in ogni caso ad adottare le misure di sicurezza che valgano ad evitare che i dati raccolti possano venire a conoscenza di terzi o possano comunque andare dispersi:

La legge distingue in proposito le misure di sicurezza da adottare in due categorie:
1. le misure di sicurezza *idonee;*
2. le misure di sicurezza *minime.*

La distinzione ha rilevanza ai fini sanzionatori, in quanto la inosservanza delle misure minime comporta una sanzione di natura penale. L'inosservanza delle misure *idonee* non comporta sanzioni ma espone ad eventuali azioni dei soggetti lesi per il risarcimento del danno.

6.1. Le misure di sicurezza "idonee"

L'obbligo di adottare misure di sicurezza *idonee* si sostanzia in un obbligo generico di predisporre qualunque precauzione necessaria alla tutela dei dati, per evitare, cioè, il rischio di distruzione o dispersione anche accidentale degli stessi ovvero di conoscenza da parte di terzi.
L'art. 31 del Codice infatti prevede che *" I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione 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."*

L'inadempienza di tale obbligo espone a responsabilità civile per danno.

L'adozione delle misure di sicurezza idonee è obbligatoria sia per i professionisti che per i Collegi provinciali.

6.2. Le misure di sicurezza "minime"

Nel quadro generale degli obblighi di sicurezza, la norma individua alcune misure di sicurezza ritenute indispensabili alla tutela dei dati personali, sono le così dette misure *minime* di sicurezza, previste dagli artt. 34 e 35 del Codice e specificate nell'allegato b) (disciplinare tecnico). Le misure minime di sicurezza sono differenziate a seconda delle modalità di trattamento dei dati:

- dati trattati senza l'ausilio di strumenti elettronici;
- dati trattati con l'ausilio di strumenti elettronici.

Il mancato adeguamento alle misure minime di sicurezza costituisce reato, con la previsione della pena dell'arresto sino a 2 anni o dell'ammenda da 10.000 50.000 € (art. 169 del Codice).

Le misure di sicurezza minime già previste avrebbero dovuto essere adottato entro il 1° gennaio 2004. Il Codice Privacy prevede che le misure minime di sicurezza di nuova istituzione debbano invece essere adottate entro il 30 giugno 2004.
Si raccomanda, pertanto, a *tutti i soggetti che trattino dati personali,* di provvedere all'adozione delle misure minime di sicurezza, quali modificate dal Codice, entro la predetta data del **30 giugno 2004**.

E' possibile richiedere una **proroga al 1° gennaio 2005** per l'adeguamento degli strumenti informatici alle misure minime di sicurezza (art. 180 del Codice sulla privacy).
La proroga può essere richiesta esclusivamente da parte dei *titolari* del trattamento dati che, alla data del 1° gennaio 2004, 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 non dovrà trasmettere alcuna istanza ma dovrà limitarsi ad elencare le motivazioni della richiesta in un apposito documento a data certa, da conservare presso la propria struttura.

L'adozione delle misure minime di sicurezza è obbligatoria sia per i professionisti che per i Collegi provinciali.

6.2.1. Dati trattati senza l'ausilio di strumenti informatici

Le misure minime di sicurezza da adottare per il trattamento dei dati personali in modo "cartaceo" (senza l'ausilio di strumenti informatici) sono tre:

1. l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
2. la previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
3. la 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.

I primi due punti riguardano il caso in cui si sia provveduto ad individuare uno o più *incaricati* del trattamento. In tale ipotesi sarà dunque necessario, così come specificato dal Disciplinare tecnico (allegato b del Codice):

- impartire istruzioni scritte agli *incaricati* specificando l'ambito del trattamento consentito. Tali istruzioni devono essere aggiornate con scadenza almeno annuale;
- quando gli atti e i documenti contenenti *dati sensibili o giudiziari* sono affidati agli *incaricati*, i medesimi atti e documenti devono essere controllati e custoditi dagli *incaricati* fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e siano restituiti al termine delle operazioni affidate.

L'ultima misura minima di sicurezza da adottare riguarda anche coloro che non abbiano designato alcun incaricato ed è posta a tutela dei locali in cui vengono conservati i dati. L'allegato b specifica in proposito che:

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

6.2.2. Dati trattati con l'ausilio di strumenti informatici

Il trattamento dati effettuato con strumenti informatici prevede l'adozione di più complesse misure minime di sicurezza. Qui di seguito ne riportiamo l'elenco:

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

Per quanto riguarda tutti i punti, ad esclusione della lettera g (Documento programmatico sulla sicurezza, che verrà analizzato a parte nel paragrafo successivo), si tratta di precauzioni da adottare sui sistemi informatici secondo le modalità prescritte dall'allegato b del Codice.

Sarà dunque opportuno rivolgersi ai tecnici che forniscono la manutenzione per i propri *computer* per farsi rilasciare un'attestazione comprovante l'adozione delle misure privacy.

6.2.2.1. Il Documento Programmatico sulla Sicurezza

Come già detto, nell'ambito delle misure minime di sicurezza da adottare per il trattamento dati con l'ausilio di strumenti elettronici, rientra anche la predisposizione del Documento Programmatico sulla Sicurezza (DPS).
Il DPS deve essere redatto entro il 30 giugno 2004. Dal 2005 dovrà essere redatto o aggiornato entro il 31 marzo di ogni anno.

Il DPS deve 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, nonché 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.

Ricordiamo che, con parere del 22 marzo scorso il Garante ha provveduto a delimitare l'ambito di applicazione dell'obbligo di redazione del DPS, stabilendo che sono tenuti all'adempimento coloro che "*trattano dati sensibili e/o giudiziari con l'ausilio di strumenti elettronici*" (in merito si veda la Circolare della Fondazione Luca Pacioli Documento n. 10 del 31 marzo 2004).
Si segnala, però, che nonostante i chiarimenti forniti dal Garante, 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. Taluni hanno tuttavia avanzato delle perplessità a proposito delle seguenti tipologie di dati trattati all'interno della dichiarazione dei redditi (trasmessa per via telematica):

1. Spese mediche
2. Destinazione dell'8 per mille

In merito al primo punto riteniamo che le spese mediche 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 del secondo punto, riteniamo anche in questo caso che i dati relativi alla destinazione dell'otto per mille non possano essere considerati dati sensibili. Infatti, sembra che nella fattispecie possa ravvisarsi esclusivamente una destinazione di risorse allo Stato piuttosto che ad una confessione religiosa, senza che alla stessa destinazione possa ricondursi in nessun modo una manifestazione di convinzione religiosa.
La Fondazione Luca Pacioli, in merito, ha chiesto chiarimenti al Garante.

In attesa che l'Autorità si pronunci, potrebbe essere opportuno ugualmente provvedere all'adempimento entro il 30 giugno al fine di precostituirsi una prova della

dovuta diligenza nella predisposizione delle misure di sicurezza, da utilizzare nel caso di eventuali pretese risarcitorie per la violazione degli obblighi di sicurezza, di cui all'art. 31 del Codice Privacy (misure di sicurezza "idonee").

7. La Privacy e il bilancio

La nuova disciplina privacy 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*". In altre parole, nella relazione accompagnatoria al bilancio di esercizio deve darsi notizia dell'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza (vedi paragrafo 6.2.2.1).

Circa tale adempimento con riferimento al bilancio relativo all'esercizio 2003, l'Autorità Garante con parere del 22 marzo scorso, ha chiarito quanto segue:

- i soggetti tenuti nel passato a predisporre o aggiornare il DPS e che per il 2004 possono aggiornarlo entro il 30 giugno 2004, dovranno applicare la disposizione del punto 26 sopra citata già a partire dalla relazione sul bilancio di esercizio per il 2003. Nel caso in cui abbiano già provveduto all'aggiornamento del DPS per il 2004, senza attendere la data del 30 giugno, dovranno darne notizia nella relazione accompagnatoria al bilancio. Viceversa, qualora non avessero ancora redatto il DPS, dovranno indicare l'avvenuto aggiornamento del DPS per l'anno 2003 ed indicare sinteticamente che si provvederà ad aggiornare il DPS entro il 30 giugno 2004;
- i soggetti tenuti per la prima volta a redigere il DPS nel 2004 (entro il 30 giugno), non devono indicare nella relazione alcunchè se il DPS 2003 o 2004 non sono stati adottati. I medesimi soggetti, qualora alla data in cui predispongono la relazione accompagnatoria abbiano già redatto il DPS 2004, indicheranno invece tale circostanza. Essi potranno infine indicare facoltativamente quanto eventualmente già fatto nel 2003 e, sempre facoltativamente, l'aggiornamento 2004 *in itinere*.

8. Tabella riassuntiva degli adempimenti ai fini di una corretta applicazione delle disposizioni sulla Privacy

DISPOSIZIONI PER LA PRIVACY	RAGIONIERI	COLLEGI
Individuazione degli eventuali responsabili ed incaricati del trattamento dati	**Facoltativa** Il titolare può individuare uno o più responsabili con compiti specificati per iscritto. Il titolare può, inoltre, individuare uno o più incaricati con nomina effettuata per iscritto e nella quale sia individuato puntualmente l'ambito del trattamento consentito.	**Facoltativa** Il titolare può individuare uno o più responsabili con compiti specificati per iscritto.Il titolare può, inoltre, individuare uno o più incaricati con nomina effettuata per iscritto e nella quale sia individuato puntualmente l'ambito del trattamento consentito.
Informativa	**Obbligatoria**	**Obbligatoria**
Consenso	**Obbligatorio** fuori dai casi previsti di esenzione (paragrafo 4.3)	**Obbligatorio** fuori dai casi previsti di esenzione (paragrafo 4.3)
Notificazione	**Esentati**	**Esentati**
Autorizzazione	**Esentati**	**Esentati**
Misure Idonee	**Obbligatorie**	**Obbligatorie**
Misure minime	**Obbligatorie**	**Obbligatorie**
DPS	In attesa di chiarimenti da parte del Garante **Consigliabile**	In attesa di chiarimenti da parte del Garante **Consigliabile**