

CIRCOLARE N. 10/2004

“Privacy”: nuovo testo unico – obblighi informativi nella relazione sulla gestione – notificazione

© Copyright 2003 Acerbi & Associati®

Come già indicato nella nostra circolare 25/2003 (in www.fiscoeimpresa.com), in data 30.06.2003 è stato emanato il Decreto Legislativo n. 196 che contiene il nuovo "Codice in materia di protezione dei dati personali" (di seguito per brevità denominato il "T.U."). **Le relative norme sono entrate in vigore in data 1.1.2004.**

Il provvedimento accorpa, integra, abroga e riscrive numerose disposizioni stratificatesi negli anni in materia di cd. "Privacy"

Particolare attenzione deve essere posta agli adempimenti in materia di **misure di sicurezza** dei dati oggetto di trattamento.

È stato concesso termine fino al **30 giugno 2004** per adeguarsi alle misure di sicurezza definite negli articoli 33, 34 e 35 dell'allegato B al nuovo T.U (sono quelle non previste dal DPR 318/99; NB: ricordiamo invece che il termine per l'adozione delle misure di sicurezza previste dal citato DPR **sono già scadute – si veda nostra circolare 10/2000 sulle misure minime di sicurezza, disponibile nella sezione iscritti di www.fiscoeimpresa.com**).

Le misure di sicurezza sono distinte a seconda che si riferiscano a trattamenti dati operati con strumenti elettronica, o rispettivamente senza l'ausilio di strumenti elettronici (trattamenti manuali e cartacei).

Nel frattempo esiste l'obbligo di garantire che i rischi a cui sono sottoposti i dati non si incrementino. La mancata adozione delle misure minime previste dall'articolo 33 è punito con **l'arresto sino a 2 anni o con l'ammenda da Euro 10.000 a Euro 50.000.**

Il reato è obblazionabile mediante il pagamento di una somma pari a 1/4 della ammenda stabilita per la contravvenzione, qualora l'autore del reato abbia provveduto a regolarizzare le misure entro l'eventuale termine (max 6 mesi) concesso a tal fine dal Garante.

Il titolare che alla data di entrata in vigore del T.U. (01.01.2004) dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'art. 34 e delle corrispondenti modalità tecniche di cui all'allegato B), deve descrivere le medesime ragioni in un apposito documento avente **data certa** da conservare presso la sede sociale.

Nel caso in cui l'adozione delle misure di sicurezza avvenga mediante soggetti esterni alla struttura aziendale, il titolare dell'azienda deve esigere e ricevere dall'installatore una descrizione scritta dell'intervento tecnico effettuato che ne attesti la conformità alle disposizioni del presente disciplinare tecnico.

E' stato generalizzato l'obbligo del DPSS (documento programmatico di sicurezza), per coloro che trattano **dati sensibili** (sono "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). Detto documento, da redigersi o aggiornarsi ogni anno entro il **31 marzo** (la prima scadenza è però il **30.06.2004**, come sopra indicato) deve contenere idonee informazioni riguardo (con riferimento ai titolari di attività diverse da quelle sanitarie):

- a) l'elenco dei trattamenti dei dati personali;
- b) la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- c) l'analisi dei rischi che incombono sui dati;
- d) le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- e) la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento, in tempi certi e non superiori a 7 giorni;

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

Si evidenzia che il trattamento di dati sensibili è comune alla maggior parte delle imprese nell'ambito della ordinaria attività di gestione del personale (e, spesso, anche della selezione dello stesso) e che, quindi la redazione del DPSS sarà normalmente dovuta. Non si deve, infatti, confondere detto obbligo con l'eventuale non necessità di chiedere il consenso dell'interessato per il trattamento dei relativi dati sensibili (ad esempio perché necessario per la gestione, appunto, del rapporto di lavoro dipendente), come meglio oltre.

Inoltre, è stato introdotto a carico degli amministratori di società l'espresso obbligo (punto n. 26 dell'allegato B al T.U.) di riferire, **nella Relazione al Bilancio d'esercizio** (leggasi la relazione sulla gestione ex art. 2428 c.c.), se dovuta (quindi non nel caso di bilancio cd. "abbreviato"), circa **l'avvenuta adozione o il successivo aggiornamento del DPSS**. Si ritiene che questo adempimento non determini la necessità di una descrizione, anche sintetica, del DPSS, **ma semplicemente dell'indicazione del fatto che il DPSS sia stato adottato o aggiornato**.

Quest'obbligo informativo risulta a nostro avviso dovuto già nella relazione sulla gestione relativa al bilancio 2003. In tal senso:

- poiché il termine ultimo per la redazione del DPSS secondo il nuovo T.U. è, come visto, il 30 giugno 2004;
- il DPSS era una delle misure di sicurezza già previste dal D.P.R. 318/1999 (cfr. art. 6), ma che il nuovo T.U. innova ed estende,

si ritiene che la relazione sulla gestione al bilancio 2003 debba indicare:

- se in vigore del D.P.R. 318/1999 il DPSS era già dovuto, l'indicazione che il medesimo documento è stato redatto, appunto, secondo la previgente disposizione ed è in corso di aggiornamento per adeguarlo al nuovo T.U.;
- se non era dovuto, nessuna indicazione.

Con riferimento al **consenso dell'interessato**, sono state introdotte procedure semplificate per la sua acquisizione. E' altresì stata confermata la necessità dell'Informativa agli interessati preventiva al trattamento dei dati. Si evidenzia che le **autorizzazioni generali del Garante per il trattamento di dati sensibili** sono in vigore, salvo proroghe, fino al **30.06.2004**. E' comunque sempre dovuta la verifica della presenza delle condizioni in base alle quali dette autorizzazioni sono state rilasciate. In caso contrario, infatti, è dovuta l'autorizzazione "ad personam" prevista già dalla vecchia normativa e confermata dal nuovo T.U. per, appunto, poter trattare dati sensibili anche nel caso in cui non sia necessario il consenso dell'interessato.

Per quanto riguarda la **notificazione**, si evidenzia che è stata semplificata e circoscritta a casi veramente particolari (cfr. art. 37 c. 1 nuovo T.U.) che non dovrebbero riguardare la maggior parte delle imprese (solo l'ipotesi di banche dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale e al corretto adempimento di obbligazioni sembra poter aprire uno "spiraglio" ad un obbligo generalizzato di notifica per le imprese, dato che tutte di fatto dispongono di dati per il monitoraggio della solvibilità dei propri clienti – ciò, però, appare in contrasto con l'estrema specificità delle altre situazioni che comportano l'obbligo di notifica, cioè le lettere da a) a e) del comma 1 dell'art. 37 del T.U.). Dal 1° gennaio 2004 non è

più utilizzabile il precedente modello di notifica. La notificazione è ora possibile solo per via telematica e con sottoscrizione con firma digitale, tramite il sito <https://web.garanteprivacy.it/rgt/> del Garante della privacy (compilando i campi del modello ivi disponibile), anche con la collaborazione di eventuali intermediari autorizzati.

Allo stato non sono previste e ammesse altre modalità. A differenza della notificazione prevista dalla legge n. 675/1996, non è quindi possibile utilizzare modelli cartacei o dischetti, né per la compilazione, né per l'invio.

Per perfezionare la notificazione diviene necessario sottoscriverla con firma digitale (art. 10, comma 3, d.P.R. n. 445/2000).

A tal fine, il titolare del trattamento deve utilizzare un dispositivo di firma digitale, disponibile presso uno dei certificatori accreditati ai sensi dell'art. 2, comma 1, lett. c), d. lg. n. 10/2002. L'elenco dei certificatori è rinvenibile sul sito www.cnipa.gov.it. La notificazione così sottoscritta, va trasmessa per via telematica al Garante.

Ogni notificazione al Garante deve essere accompagnata dal pagamento dei diritti di segreteria, il cui importo è fissato in euro 150,00.

Il pagamento è possibile on line mediante carta di credito su protocollo sicuro; altre modalità sono: bonifico bancario, conto corrente postale, banco posta; per questi casi occorre indicare gli estremi del pagamento nell'apposito riquadro. Le coordinate bancarie per il pagamento sono: c.c. 000000018373 intestato a "Garante per la protezione dei dati personali" - ABI 05164 - CAB 03202 - presso Banca Popolare di Lodi, ag. n. 2 di Roma, via Bevagna, 24, 00191 Roma.

Il pagamento anche può essere effettuato sul c.c. postale n. 97204002 intestato a "Garante per la protezione dei dati personali", Piazza di Monte Citorio, 115/121, 00186, Roma, indicando come causale "diritti di segreteria per notificazione".

Il Garante invierà all'indirizzo di posta elettronica indicato dal notificante un messaggio di conferma del ricevimento della notificazione che attesta il buon esito della procedura.

È possibile stampare copia della notificazione; tale copia cartacea, comunque, non deve essere trasmessa al Garante.

Come detto, dal 1° gennaio 2004 sono tenuti a notificare solo i titolari che effettuano una o più attività di trattamento tra quelle specificamente indicate dal Codice (art. 37 del Codice) o dal Garante con appositi provvedimenti (allo stato non adottati)

La precedente normativa, invece, prevedeva per tutti i titolari l'obbligo di effettuare la notificazione, a meno che potessero avvalersi dei casi di esonero o di possibile utilizzazione di una notificazione semplificata).

Il titolare che non è tenuto alla notificazione deve comunque fornire le notizie contenute nel modello di notificazione a chi ne fa richiesta (nell'esercizio del diritto di accesso e degli altri diritti riconosciuti all'interessato), a meno che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

Il titolare che abbia già iniziato un trattamento anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che lo abbia notificato in passato, deve procedere, se vi è tenuto, alla nuova notificazione entro il 30 aprile 2004 (art. 181, comma 1, lett. c)).

Alcuni operatori che iniziano ex novo una nuova attività di trattamento dei dati a partire dal 1° gennaio potrebbero essere altresì tenuti alla previa notificazione.

In caso di contitolarità del trattamento, ciascun contitolare è tenuto ad effettuare un'autonoma notificazione, nella quale indicherà tutti gli altri contitolari. Ciascun titolare sottoscriverà pertanto solo la propria notificazione.

Per gli operatori è consigliabile approfondire attentamente i contenuti del nuovo modello di notificazione telematica, prima di procedere a questo importante adempimento.

Chi esegue la notificazione secondo la nuova procedura, deve dichiarare che effettua una "nuova notificazione", anche nel caso in cui in passato abbia già presentato una notificazione in base alla legge n. 675/1996.

Ulteriori eventuali notificazioni costituiscono "modifiche del trattamento", oppure "cessazione del trattamento" (nel caso in cui l'intero trattamento precedentemente notificato venga a cessare definitivamente).

Per quanto riguarda la modifica della notificazione, è sufficiente che il notificante richiami a video la notificazione già trasmessa, apportando le modifiche per i soli riquadri interessati. La notificazione, così modificata, è trasmessa osservando la medesima procedura telematica ora prevista per la "nuova notificazione".

Nel caso di notificazione omessa, ritardata o incompleta, il titolare è punito con sanzione pecuniaria (da diecimila euro a sessantamila euro) e con la pena accessoria della pubblicazione dell'ordinanza che applica la sanzione stessa in uno o più giornali, per intero o per estratto.

La falsa dichiarazione è inoltre un reato, punito con la reclusione (da sei mesi a tre anni e salvo che il fatto configuri un reato più grave).

Le notificazioni sono inserite in un registro pubblico consultabile gratuitamente da tutti on-line (ad esempio, per esercitare il diritto di accesso ai dati o altri diritti riconosciuti dal Codice in materia di protezione dei dati personali).

Mediante il registro saranno effettuati controlli sui trattamenti oggetto di notificazione, verificando le notizie in essa contenute.

Il Garante stipulerà apposite convenzioni con soggetti qualificati (di seguito denominati "intermediari"), presso i quali sarà possibile la sottoscrizione della notificazione con firma digitale **laddove il notificante non fosse in possesso del dispositivo di firma digitale.**

Al momento il Garante ha stipulato una prima convenzione con Poste italiane Spa per permettere l'inoltro della notificazione tramite gli uffici PT business. La convenzione ha la durata di un anno a partire dal primo gennaio 2004 e verrà attivata entro i primi di gennaio. Tale servizio ha un costo massimo di euro 25,00, che l'utente paga direttamente all'operatore.

Infine, segnaliamo la necessità di approfondire le disposizioni di cui agli artt. 9 e 10 del D.Lgs. 276/2003 (cd. "riforma Biagi", in vigore dal **24 ottobre 2003**) in materia di **ricerca e selezione del personale**, che impongono ai datori di lavoro il rispetto di alcuni nuovi requisiti in fase di acquisizione di dati personali dei candidati ad un rapporto di lavoro. In particolare la legge richiede che non vengano raccolti né trattati dati personali "non strettamente attinenti alle attitudini professionali e all'inserimento lavorativo" dei lavoratori. Ad es. quelli relativi allo stato matrimoniale e di famiglia.

Spesso nella modulistica utilizzata a tal scopo, viceversa, si rinviene la presenza di numerosi campi riferibili a tali tipi di dati non pertinenti ma soprattutto non più ammissibili secondo la nuova normativa.

Nell'ambito di Acerbi & Associati la materia della "privacy" è seguita dall'Avv. De Muri, che è a Vs. disposizione per consulenze, analisi e interventi. Data l'importanza delle sanzioni previste in caso di non ottemperanza agli obblighi stabiliti dalla normativa in questione, Vi invitiamo a non sottovalutare la portata della stessa. Solo da opportune valutazioni, inoltre, possono risultare applicabili procedure e trattamenti semplificati.

Stiamo allo scopo predisponendo specifiche "check list" che saranno messe a disposizione di chi vorrà effettuare un primo monitoraggio della situazione allo scopo di verificare le eventuali azioni da intraprendere.