

MINISTERO DELL'UNIVERSITA' E DELLA RICERCA - UFFICIO SCOLASTICO REGIONALE PER LA PUGLIA
ISTITUTO COMPRENSIVO STATALE con sezione musicale
SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA DI 1° GRADO

"MUSTI-DIMICCOLI" - Barletta



Piano Operativo Privacy

del 31 marzo 2006

E' stato pubblicato in Gazzetta Ufficiale il Codice in materia dei dati personali che entrerà in vigore il 1° gennaio 2004 e sostituirà la legge n. 675/1996 e molte altre disposizioni transitorie di legge e di regolamento. Al fine di evitarvi inutili spese riportiamo di seguito un estratto delle principali **misure da adottare** e dei **documenti da predisporre e conservare** ricordando che per quel che concerne gli adeguamenti informatici e tecnici sarà necessario, per chi non è in grado di operare direttamente, rivolgersi ai propri tecnici di fiducia. In relazione alla tempistica nell'espletamento di quanto richiesto per l'adeguamento alle c.d. "misure minime di sicurezza", il codice della Privacy fissa quale data ultima quella del 31.03.2006. Successivamente a tale data ogni infrazione al suddetto Codice comporterà non solo sanzioni amministrative (che vanno da un minimo di 3.000 € esempio per la mancata informativa all'interessato fino ad un massimo di 60.000 € esempio per la mancata notifica al garante, sanzioni che in alcuni casi possono essere anche triplicate) ma anche la possibilità, in caso di denuncia da parte di dipendenti e/o terzi, di sanzioni penali che potranno comportare la reclusione addirittura fino ai tre anni.

Procediamo quindi qui di seguito ad elencare passo per passo tutte i punti da espletare ricordando che la normativa sulla privacy disciplina il trattamento dei dati personali (siano essi di persona fisica e/o giuridica), anche detenuti all'estero, effettuato da qualsiasi professionista, imprenditore individuale, persone giuridica, pubblica amministrazione e da qualsiasi altro ente, associazioni ed organismo. Restano quindi escluse le persone fisiche che trattino dati personali di altri per fini esclusivamente personali.

N.B.

più avanti si potrà far riferimento ai c.d. "dati sensibili": si ricorda che tali dati sono identificati come tutti quei 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.

PUNTO 1° - NOTIFICA AL GARANTE

Nei casi di particolare trattamento di dati sensibili (art. 37 del Codice della Privacy), gli stessi saranno possibili solo previa autorizzazione da parte del Garante (massima autorità in materia di sicurezza della privacy). Tale notifica dovrà essere resa entro e non oltre il **31.03.2006** o comunque entro l'inizio del trattamento dei dati stessi quando successivo a tale data (es. nuove società). Il Garante risponde entro **45 giorni** decorsi i quali la mancata pronuncia equivale a rigetto. Il nuovo Codice della privacy ha previsto una serie di semplificazioni, alcune delle quali proprio in merito all'eliminazione dell'obbligo generale di notifica e lo ha fatto prevedendo alcune ipotesi di esonero tra le quali si ricorda:

- il trattamento dei dati comuni necessario per l'assolvimento di un compito previsto dalla legge, regolamento, normativa comunitaria;
- il trattamento riguardante dati contenuti o provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

- il trattamento riguardante rubriche telefoniche o analoghe non destinate alla diffusione, utilizzate esclusivamente per ragioni di ufficio e di lavoro e comunque per **fini diversi dall'invio di materiale pubblicitario**;
- il trattamento finalizzato esclusivamente all'adempimento di specifici obblighi contabili, retributivi, previdenziali, assistenziali e fiscali, purché effettuato con riferimento alle sole categorie di dati, di interessati, e di destinatari della comunicazione o diffusione strettamente collegate a tale adempimento, conservando i dati non oltre il periodo necessario all'adempimento o previsto per legge (es. ex dipendenti).

Tali esoneri dovrebbero essere sufficienti per evitare la notifica nella maggior parte dei casi.

PUNTO 2° - INFORMATIVA

La persona fisica o giuridica di cui si trattano i dati ha il diritto di essere informato sia del trattamento stesso sia dei modi e delle finalità per cui è effettuato. Tale informativa (che la legge prevede possa essere anche resa verbalmente, metodo che però non appare sufficientemente sicuro), deve essere fatta firmare ogni qual volta si entri in contatto per la prima volta con un nuovo cliente, dipendente, collaboratore ecc.. L'informativa dovrà essere resa anche **ai fornitori** che a loro volta la raccolgono da noi e vanno conservate fino a che si conservano i dati relativi all'interessato. Resta comunque valida (specialmente quando si corre il rischio di dimenticarsi della raccolta di un'informativa preventiva) l'adozione di una apposita frase direttamente in fattura pertinente solo alla fase di vendita.

L'informativa dovrà essere resa anche **ai dipendenti** facendo però presente che solitamente tale informativa è predisposta e conservata dal consulente delle paghe e che sarà quindi meglio contattarlo prima di procedere all'espletamento di tale onere.

PUNTO 3° - IDENTIFICAZIONE DEL TITOLARE DEL TRATTAMENTO

L'amministratore e/o il titolare della ditta/studio deve redigere un documento in cui la ditta/società o il titolare stesso venga identificato come "**Titolare del trattamento**" di tutti i dati in suo possesso da chiunque forniti. Nel documento redigerà un elenco degli archivi cartacei ed elettronici (nel documento da noi predisposto trovate un esempio nella tabella) conservati spiegando anche il metodo di archiviazione di tali dati. Alla fine della compilazione di questo documento alleghiamo, oltre al fac-simile, un elenco di codici predisposti dal Garante da usarsi per definire: il tipo di titolare, il tipo di dati comuni e/o sensibili utilizzati e le finalità per le quali vengono usate.

PUNTO 4° - NOMINA DEL TITOLARE DEL TRATTAMENTO

Il titolare del trattamento di cui al punto precedente nominerà uno o più responsabili i quali vigileranno sul corretto utilizzo degli archivi e sulla loro conservazione. La nomina del responsabile è facoltativa ma è bene che l'Amministratore unico, il Presidente del C.d.A. o il legale rappresentante venga nominato a questo incarico al fine di evitare che eventuali responsabilità possano ricadere sui dipendenti e/o collaboratori che si occupano quotidianamente del trattamento dei dati ai fini contabili-fiscali.

PUNTO 5° - ADOZIONE MISURE DI SICUREZZA

Entro il 31.03.2006, dovranno essere adottate le misure minime di sicurezza previste dal disciplinare tecnico allegato al Codice della Privacy. Tali misure possono essere così adempiute:

Nomina degli incaricati al trattamento dei dati

Il Responsabile del trattamento nominerà e autorizzerà per iscritto tutte le persone addette all'utilizzo degli archivi cartacei e/o elettronici. L'autorizzazione potrà essere generale o limitata ad alcuni specifici dati e programmi e dovrà essere rilasciata prima dell'inizio del trattamento.

Tali autorizzazioni dovranno essere verificate almeno una volta l'anno e se necessario modificate (es. contabile amministrativo che viene promosso a responsabile vendite/acquisti ecc.). Verrà poi redatto un apposito elenco di tutti gli incaricati che comprenderà, dove sia utilizzata una rete di computer, lo User-Id che identifica il PC utilizzato da ognuno.

Ad ogni incaricato dovranno essere assegnate delle password **univoche e non riutilizzabili** sia per entrare all'interno del programma sia per riprendere l'uso del pc dopo essersi allontanato (c.d. screen-saver). Tali password, che dovranno essere di almeno otto caratteri, dovranno essere conservate diligentemente da ogni incaricato e dallo stesso modificate almeno ogni sei mesi (ridotti a tre per gli incaricati al trattamento dei dati sensibili). Le password non utilizzate da almeno 6 mesi (es. maternità di un dipendente) e quelle non più utilizzate (es. ex dipendente) devono essere disattivate.

Custode delle Password

Il Responsabile del trattamento nominerà un Custode delle Password che sarà l'unico a conoscere tutte le password, oltre naturalmente al singolo incaricato che sarà a conoscenza solo della propria, e provvederà a controllare che le password siano univoche. Egli predisporrà tante buste chiuse quanti sono gli incaricati al trattamento. Tali buste, riconoscibile all'esterno da nome dell'incaricato, conterranno le password (vedi documento 6bis) e dovranno essere custodite in posto sicuro e non accessibile. Quando uno o più incaricati dovessero variare, il Custode provvederà a distruggere la/le relativa/e buste ed eventualmente, se necessario, a predisporre delle nuove per i nuovi incaricati ricordandosi sempre che una parola chiave già utilizzata non può essere riassegnata ad un nuovo utente. Il procedimento fin qui descritto deve essere effettuato anche in presenza di un solo PC.

Amministratore di sistema

Dove sia utilizzata una rete o vi siano più elaboratori, è necessario che il Responsabile nomini un Amministratore di sistema incaricato del controllo dei trattamenti effettuati elettronicamente. L'Amministratore di sistema provvederà anche, ogni sei mesi al massimo, ad archiviare un documento da lui firmato e datato in cui segnalerà quanto fatto al fine dell'adeguamento e/o dell'aggiornamento dei sistemi antivirus. Provvederà inoltre, in presenza di dati sensibili, ad adottare idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici nel tempo massimo previsto in sette giorni.

Ove, per mancanza dei presupposti, non si renda necessaria la nomina di un amministratore di sistema, il documento relativo agli antivirus dovrà comunque essere compilato e conservato a cura di uno dei responsabili del trattamento.

Back-up

Dove esista trattamento dei dati effettuato tramite elaboratore vi è l'obbligo di provvedere ad effettuare, con frequenza almeno settimanale, copie di sicurezza ed a redigere un documento che spieghi il sistema utilizzato per effettuare tali copie.

Accessi ai locali

Il Responsabile del trattamento nominerà uno o più responsabili all'accesso dei locali adibiti a conservazione cartacea e/o elettronica delle banche dati. Ove esista un custode notturno, questo sarà nominato quale responsabile dei locali specificando nel documento che l'incarico gli viene affidato per le ore di chiusura degli uffici.

PUNTO 6° - DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Entro il 31 marzo di ogni anno ed in presenza di dati sensibili, il titolare del trattamento dovrà redigere un documento programmatico sulla sicurezza in cui verranno elencati tutti i provvedimenti presi e gli adeguamenti effettuati al fine della tutela sulla Privacy.

Il Titolare dovrà inoltre **riferire** della redazione o dell'aggiornamento di tale documento **nella relazione accompagnatoria al bilancio** (quando prevista).

PUNTO 7° - INTERVENTI IN ESTERNO

Quando per l'espletamento delle misure minime di sicurezza ci si avvalga della collaborazione di soggetti esterni, sarà necessario farsi rilasciare da questi ultimi una descrizione scritta dell'intervento o dell'aggiornamento effettuato da cui ne risulti la conformità alle disposizioni di legge.

* * * *

Tutti i documenti su elencati dovranno essere custoditi in luogo sicuro e aggiornati secondo necessità. Ogni titolare del trattamento dovrà inoltre provvedere a:

- procurarsi, se già non l'avesse, archivi muniti di serratura dove conservare i documenti cartacei o in alternativa predisporre quale archivio un'apposito locale sempre munito di serratura;
- se utilizza sistemi elettronici munirsi di un sistema di back-up (copie di sicurezza), di un gruppo di continuità, di una messa a terra e di un sistema antivirus con licenza;
- adottare un sistema antincendio e un allarme antifurto.

Consigliamo inoltre a tutti, per una maggior tutela, di:

- allegare ad ogni fax un'apposita frase tutelativa in caso d'errore di ricezione che potrà essere così predisposta: "Qualora questo messaggio fosse da Voi ricevuto per errore vogliate cortesemente darcene notizia a mezzo telefax oppure e-mail e distruggere il messaggio ricevuto erroneamente. Quanto precede ai fini del rispetto della Legge 675/96 sulla tutela dei dati personali";
- fare attenzione ad ogni spedizione e-mail effettuata tenendo presente che, quando vi sono più destinatari di uno stesso messaggio, è necessario, al fine di evitare la diffusione degli indirizzi di posta elettronica, procedere con il seguente metodo: inserire nel rigo di destinazione "A: " il proprio indirizzo; inserire l'elenco vero e proprio dei destinatari nel rigo identificato da "Ccn: ".

Per le società che oltre all'amministratore non abbiano altro collaboratore né alcun dipendente saranno da predisporre solo i documenti n. 1 e n. 3 e, quando necessario, il n. 10 avendo però cura di integrare la nomina del titolare con tutte le autonomie necessarie alle proprie banche dati e il documento programmatico con le spiegazioni del caso.

Il Responsabile della Sicurezza Informatica
