Codice in materia di protezione dei dati personali

Decr. Legislativo n.ro 196 del 30 Giugno 2003

Guida di approfondimento

Soft.Com

SOME RIGHTS RESERVED

© 2005 **Filippo Cerulo** – Soft.Com Sas
www.softcombn.com - email: filippo.cerulo@softcombn.com

Quest'opera è rilasciata sotto la licenza *Creative Commons*
"Attribuzione - Non commerciale - Non opere derivate 2.0 Italia."

Per visionare una copia di questa licenza visita il sito web
http://creativecommons.org/licenses/by-nc-nd/2.0/it/ o richiedila per posta a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, Usa.

Tu sei libero:

- di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire o recitare l'opera

Alle seguenti condizioni:

Attribuzione. Devi riconoscere il contributo dell'autore originario.

Non commerciale. Non puoi usare quest'opera per scopi commerciali.

Non opere derivate. Non puoi alterare, trasformare o sviluppare quest'opera.

- In occasione di ogni atto di riutilizzazione o distribuzione, devi chiarire agli altri i termini della licenza di quest'opera.
- Se ottieni il permesso dal titolare del diritto d'autore, è possibile rinunciare ad ognuna di queste condizioni.

Le tue utilizzazioni libere e gli altri diritti non sono in nessun modo limitati da quanto sopra

Indice generale

Codice in materia di protezione dei dati personali..... 4
Guida di approfondimento..... 4
Premessa..... 4
Definizione delle Tipologie dei Dati (Art. 4)..... 4
Diritti di accesso ai Dati personali (Art. 7)..... 5
Informativa (Art. 13)..... 5
Richiesta del Consenso (Art. 18)..... 6
Diffusione dei Dati (Articoli 19, 20, 21 e 22)..... 6
Obblighi di sicurezza (Articolo 31)..... 7
Misure minime di sicurezza (Articoli 33, 34, 35)..... 7
Allegato B..... 8
Sistema di autenticazione informatica..... 8
Sistema di Autorizzazione..... 9
Altre misure di sicurezza..... 9
Documento Programmatico Sulla Sicurezza (DPSS)..... 10
Ulteriori misure in caso di trattamento di dati sensibili o giudiziari..... 10
Misure di tutela e garanzia..... 10
Trattamenti senza l'ausilio di strumenti elettronici..... 11
Considerazioni sulla stesura del DPSS..... 11
Conclusioni..... 12

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

Codice in materia di protezione dei dati personali

Guida di approfondimento

Premessa

L'entrata in vigore del Codice in materia di protezione dei Dati personali ha posto gli Enti e le Aziende di fronte ad una serie di obblighi riguardanti i trattamenti elettronici e cartacei delle informazioni. Questa guida ha lo scopo di approfondire alcuni aspetti della normativa con specifico riferimento alle Scuole Pubbliche.

Definizione delle Tipologie dei Dati (Art. 4)

La prima, ovvia, domanda è **quali Dati tratta la Scuola, e di che tipo ?**

Dobbiamo quindi riferirci all'**Articolo 4**, che definisce in dettaglio l'ambito di applicazione della Legge. In particolare, al comma 1, lettera a, viene definito:

- *"**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;*

Dunque la Scuola "tratta" dei dati. Ma di che tipo ? Al **comma 1**, **lettera b**, leggiamo la definizione di :

- *"**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;*

ed al c**omma 1**, **lettera d**:

- *"**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,*

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

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;

Risulta dunque ovvio che **la Scuola "tratta" sicuramente sia "Dati personali" che "Dati sensibili"**. Bisogna anche considerare, per meglio comprendere il seguito la definizione di:

- *"**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;*

Diritti di accesso ai Dati personali (Art. 7)

Il **comma 1** dell'**Articolo 7** recita:

- *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.*

Il seguito dell'**Articolo 7**, ed i seguenti **Articoli 8**, **9** e **10** descrivono nel dettaglio quali informazioni mettere a disposizione dell'interessato, e le modalità di esercizio del diritto citato. **Sarà dunque necessario provvedere a stabilire delle procedure amministrative che consentano all'interessato di accedere alle informazioni che lo riguardano.**

Informativa (Art. 13)

L'**Art. 13** prevede, al **comma 1**, che:

- *L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa: [...omissis]*

Quindi la normativa prevede che, nel momento della raccolta di dati personali, il soggetto sia informato circa alcuni aspetti del trattamento. L'informazione può essere anche orale, ma ovviamente è preferibile una forma scritta. **Sarà necessario quindi predisporre un documento da consegnare all'interessato al momento della raccolta dei dati.** Il seguente **comma 4** prevede anche il che :

- *Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.*

Quindi sembrerebbe che sia necessario informare il soggetto interessato anche quando i dati non sono raccolti direttamente. Fortunatamente il successivo comma 5, dice che:

- *La disposizione di cui al comma 4 non si applica quando:*
- *a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;*

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

Quindi, posto che la Scuola tratti solo dati in base ad un obbligo previsto dalla Legge, questo passaggio non è necessario.

Richiesta del Consenso (Art. 18)

La legge prevede che in molti casi l'interessato debba esprimere un consenso al trattamento dei Dati personali o sensibili. **La Scuola però non deve richiedere alcun consenso**, in quanto l'**Articolo 18**, al **comma 4** dice che :

- *Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.*

Diffusione dei Dati (Articoli 19, 20, 21 e 22)

Questa parte della legge regolamenta il trattamento e la diffusione dei dati trattati in base alla tipologia dei dati stessi. L'istituzione scolastica quindi deve porre sufficiente attenzione alle modalità con cui dati oggetto di trattamento possano essere conservati, trasferiti o divulgati. In particolare, riportiamo:

Il **comma 1** dell'**Articolo 19**:

- *Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.*

Il **comma 1** dell'**Articolo 20**:

- *Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.*

Il **comma 3** dell'**Articolo 22**:

- *I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.*

Questo significa che in linea di massima i dati sensibili andrebbero trattati, ove possibile, in maniera anonima (cosa che ovviamente pone notevoli difficoltà....).

Il **comma 6** dell'**Articolo 22**:

- *I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.*

Questo comma è fondamentale per comprendere quanto delicato sia il trattamento dei dati "sensibili". Il comma, infatti, pone dei seri limiti sulle modalità di gestione "informatica" dei

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

dati, indicando restrizioni tanto efficaci quanto, nella pratica, di difficile adozione. Esamineremo nel seguito, quando si parlerà dell"Allegato B", tutti i dettagli.

Il **comma 7** dell'**Articolo 22**:

- *I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.*

Quindi i dati "sanitari" (che spesso la Scuola si trova a gestire), devono essere "fisicamente" separati da quelli "personali". Nel comma 6 si parla inoltre di rendere *temporaneamente inintelligibili* tali dati, comunque *trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni,* anche nel caso di trattamento cartaceo. **La Scuola dovrebbe quindi predisporre particolari procedure per la gestione di queste tipologie di informazioni.**

Il **comma 8** dell'**Articolo 22**:

- *I dati idonei a rivelare lo stato di salute non possono essere diffusi.*

Obblighi di sicurezza (Articolo 31)

- *I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base 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.*

Questo Articolo introduce i principi generali che saranno oggetto delle indicazioni successive riguardanti il DPSS e le misure minime.

Misure minime di sicurezza (Articoli 33, 34, 35)

Articolo 33 :

- *Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.*

Articolo 34, comma 1:

- *Il trattamento di dati personali effettuato con **strumenti elettronici** è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: [... omissis]*

Articolo 35, comma 1 :

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

- *Il trattamento di dati personali effettuato **senza l'ausilio di strumenti elettronici** è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime: [... omissis]*

Quindi il trattamento dei dati personali, con o senza strumenti elettronici, è consentito a patto di rispettare precise indicazioni, esposte in generale negli articoli citati, ed in particolare nell'Allegato B, che è soggetto ad aggiornamento periodico in funzione dell'evoluzione tecnologica.

Allegato B

L'Allegato B si occupa di definire nel dettaglio le specifiche tecniche e le procedure da adottare nella trattazione dei dati sensibili, sia con l'ausilio di strumenti elettronici (ed è la parte più importante), sia senza. Nell'allegato, inoltre, troviamo anche la descrizione e le modalità di stesura del Documento Programmatico Sulla Sicurezza (DPSS).

Sistema di autenticazione informatica

La **prima regola** dell'allegato fissa subito pesanti restrizioni:

- *Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.*

Quindi è necessario un **sistema di autenticazione**, ma non basta. Se vogliamo rispettare il già citato Articolo 31, il sistema di autenticazione deve essere "forte", ossia non facilmente superabile. Quindi la prima domanda è : quale sistema di autenticazione adottare ?

Si tratta di una questione affatto banale, perché su di essa si fonda l'intero impianto della legge. Il sistema di autenticazione, inoltre, è strettamente correlato al Sistema Operativo in uso sull'elaboratore. Con queste premesse, al momento gli unici Sistemi Operativi di larga diffusione che garantiscono un sistema di autenticazione adeguato sono Windows 2000, Windows 2003, Windows XP, Linux. **Quindi ogni trattamento di dato personale o sensibile non è più possibile su Computer forniti di Windows 95, Windows 98, Windows Me**.

La stessa Microsoft, in un suo documento ufficiale riguardante il DPSS sostiene che:

I sistemi operativi della famiglia Windows 9X non prevedono sistemi di autenticazione "nativi"; viceversa i SO successivi (Windows NT, Windows 2000, Windows XP, Windows Server 2003) sono dotati di sistemi di autenticazione ed autorizzazione completi che permettono non solo l'utilizzo di user-id e password, ma anche credenziali di autenticazioni "forti" quali token o device di riconoscimento biometrico.

.....

I requisiti di sicurezza richiesti dal Codice per le user-id e password possono essere completamente rispettati mediante l'utilizzo dei sistemi operativi di ultima generazione quali

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

Windows XP e Windows Server 2003; in particolare si evidenzia che attraverso queste tecnologie è possibile rispettare le prescrizioni del codice in materia di protezione dei dati.

Le successive regole, fino alla 11, descrivono in dettaglio le caratteristiche peculiari del Sistema di Autenticazione. Queste regole vanno implementate nel Sistema Operativo scelto, cioè non basta adottare ad esempio Windows 2000; bisogna fare in modo che sia configurato seguendo le istruzioni dell'Allegato B.

Sistema di Autorizzazione

La **regola 12** prevede che:

- *Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.*

Questo significa che, se il sistema prevede che un utente già autenticato debba avere autorizzazioni diverse a seconda del proprio profilo professionale (cioè possa eseguire solo alcuni compiti, e quindi possa avere accesso solo a determinate banche dati), bisogna istituire anche un secondo livello di "autorizzazione". Quindi in primo luogo l'utente deve essere "**autenticato**", cioè "riconosciuto" dal sistema informatico, e quindi "**autorizzato**" ad accedere ai dati di propria competenza. Perciò non solo il Sistema Operativo deve prevedere una autenticazione "forte", ma anche ogni singola applicazione che tratta dati personali o sensibili deve comprendere un sistema di autorizzazione "forte", altrimenti non è conforma alla legge.

Altre misure di sicurezza

La **regola 16** prevede che :

- *I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.*

Qui ovviamente si fa riferimento ad Antivirus, SpyWare, Firewalls. Diventa dunque obbligatorio adottare sui PC programmi che impediscano l'intrusione di terzi (firewall), il danneggiamento dei dati (virus), e l'uso improprio del sistema (ancora virus e spyware). A seconda della configurazione del sistema e delle modalità di collegamento ad Internet bisogna quindi studiare soluzioni per la salvaguardia dei dati. La previsione di un aggiornamento almeno semestrale è ovviamente non realistica, in quanto ad esempio le firme degli Antivirus vanno aggiornate almeno settimanalmente.

La **regola 17** si occupa dell'aggiornamento del Sistema Operativo e delle falle di sicurezza:

- *Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.*

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

Anche in questo caso la previsione dell'aggiornamento semestrale è irrealistica : le falle di sicurezza di Windows vanno "chiuse" entro massimo un mese dal rilascio della correzione da parte di Microsoft. Bisogna quindi stabilire regole precise per l'aggiornamento delle Stazioni di Lavoro.

Documento Programmatico Sulla Sicurezza (DPSS)

La **regola 19** prevede che :

- *Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo: [... omissis]*

Seguono nel dettaglio le indicazioni precise sulle informazioni da includere nel documento.

Sul Sito del Garante della Privacy è disponibile una "Guida Operativa per redigere il Documento Programmatico sulla Sicurezza", che può (anzi deve) essere presa come base di partenza per la redazione.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

Regola 21:

- *Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.*

Quindi i supporti magnetici di Backup (su cui sono registrate le copie di sicurezza) devono essere adeguatamente protetti.

Regola 23 :

- *Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.*

Cioè in caso di problemi i dati devono essere di nuovo disponibili entro sette giorni. Questo implica la definizione di una dettagliata procedura per le copie di sicurezza ed il ripristino dei dati.

Misure di tutela e garanzia

Regola 25 :

- *Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.*

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

Quindi le Scuole, che sicuramente non hanno al proprio interno le conoscenze tecniche necessarie alla corretta applicazione della normativa, dovranno utilizzare consulenti esterni e pretendere una dichiarazione di conformità.

Trattamenti senza l'ausilio di strumenti elettronici

Questa parte dell'Allegato B descrive le procedure da seguire per il trattamento "cartaceo" dei dati. Particolare attenzione va posta nella individuazione dei trattamenti autorizzati in base alla classe di appartenenza dell'incaricato. In ogni caso è necessario prevedere procedure scritte ed istruzioni dettagliate da impartire ad ogni incaricato, secondo il suo profilo di autorizzazione.

Considerazioni sulla stesura del DPSS

Abbiamo già detto che l'Allegato B alla regola 19 descrive il contenuto del DPSS, e che il Garante ha reso disponibile un documento di Guida alla redazione. Questa Guida è piuttosto schematica, ma sicuramente logica e lineare nella descrizione delle informazioni che bisogna includere. Il rischio, in questi casi, è la prolissità. Riteniamo infatti non indispensabile una descrizione dettagliata delle "procedure" (cioè del flusso delle informazioni) che riguardano il trattamento. Piuttosto è necessario individuare con precisione **quali** dati si trattano (regola 19.1), e **chi** li tratta (regola 19.2); il "come" si trattano non è importante perché si suppone che sia conforme alla legislazione esistente. Nell'ambito delle definizioni delle procedure e degli incarichi si può scendere più nel dettaglio, ma riteniamo che il DPSS sia un documento di sintesi.

Molta più attenzione deve essere dedicata alla **analisi dei rischi** (regola 19.3) ed alle **misure** indicate nella regola 19.4. In particolare queste misure sono **prevalentemente di carattere informatico** e devono rispettare le altre regole dell'Allegato B. Infatti i rischi da contrastare, a nostro parere, riguardano soprattutto l'ambito di trattamento con strumenti elettronici e non le procedure manuali. Una dettagliata descrizione nel DPSS, ad esempio, dei locali ed addirittura degli armadi contenenti i dati cartacei dovrebbe essere continuamente aggiornata in funzione delle variazioni, a volte sostanziali, della struttura logistica dell'istituto. Perciò le "carte" devono certo essere considerate importanti, ma il rischio di accesso non autorizzato è minimo se si adotta qualche semplice regola dettata dal buon senso. Diverso è il discorso per un archivio informatico: un programma od un utente non autorizzato possono trasferire e sottrarre in un colpo solo TUTTI i dati sensibili ad esempio presenti sul Server di Istituto, causando un gravissimo danno.

Particolare attenzione inoltre deve essere posta nella programmazione della **formazione del personale** (Regola 19.6). Una corretta conoscenza di poche e semplici regole mette al riparo la struttura da danni ingenti. L'incompetenza o la negligenza di un incaricato, che ad

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com

esempio rende nota a terzi la propria password, mette in una posizione di alto rischio tutte le banche dati a cui l'incaricato stesso ha accesso.

Conclusioni

Le incombenze derivanti dall'entrata in vigore del Decreto Legislativo 196/2003 vengono vissute da molti come una ulteriore inutile complicazione del proprio lavoro. Riteniamo invece che questo sia lo strumento attraverso il quale si può prendere coscienza della importanza del dato "personale" nella società dell'informazione. La disponibilità di enormi capacità di calcolo a costi irrisori permette l'analisi incrociata di miliardi di informazioni; quando queste informazioni sono "personali" od addirittura "sensibili" il rischio per la propria privacy è altissimo. Dunque è indispensabile trattare i dati con la massima attenzione; se questo poi implica una migliore conoscenza delle tecniche di difesa "informatiche" che possono tornare utili in tanti altri ambiti, meglio ancora. Queste "misure minime di sicurezza" quindi serviranno non solo a proteggere la privacy, ma anche a migliorare l'efficienza della propria struttura.

© Filippo Cerulo - Soft.Com Sas – www.softcombn.com - email: filippo.cerulo@softcombn.com