# ISTITUTO COMPRENSIVO STATALE
# "Selvazzano Dentro II - M. Cesarotti"

# Il Codice della Privacy

## Informativa n. 02 al Personale di segreteria in servizio

# INTRODUZIONE

Il Codice della privacy rappresenta il primo tentativo al mondo di sistematizzazione delle norme in materia:

- Introduzione di nuove garanzie per i cittadini;
- Razionalizzazione delle norme esistenti;
- Semplificazione degli adempimenti;
- Sostituzione della legge madre n. 675/1996.

Nell'art. 7 del Codice, che tutela la riservatezza, si rispecchia principalmente il momento individualistico di un potere giuridico, che spetta ad ogni persona, che si esaurisce sostanzialmente nell'escludere dalla propria vita privata interferenze esterne.

Invece la protezione dei dati si concretizza nei poteri di intervento ad ogni soggetto nei confronti di chiunque gestisca informazioni personali che possono comportare impatto sociale. Nel primo caso la tutela è statica, mentre nel secondo consente di seguire e controllare la circolazione dei dati personali e la loro protezione nei diversi circuiti in cui possono venire inseriti.

Il Codice ha introdotto uno strumentario di nuove garanzie relativamente alle comunicazioni elettroniche nelle quali il diritto alla protezione dei dati non va inteso come un guscio protettivo dell'individuo, ma riguarda l'individuo nella sua proiezione nei cicli di sviluppo economico-sociale.

Il codice è diviso in tre parti:

- La prima parte è dedicata alle disposizioni generali, ordinate in modo da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato.
- La seconda parte è dedicata a settori specifici. Essa, oltre a disciplinare aspetti specifici, introduce la disciplina per il settore sanitario e quella dei controlli sui lavoratori.

- La terza parte affronta la materia della tutela amministrativa e giurisdizionale con il consolidamento delle sanzioni amministrative e penali e con le disposizioni sull'ufficio del garante.

## IL DIRITTO ALLA RISERVATEZZA NELL'ORDINAMENTO COSTITUZIONALE

Non esiste nel sistema costituzionale una norma espressa che appresti tutela generale alla riservatezza.

Per contro la costituzione riconosce espressamente alcune libertà che possono atteggiarsi al limite della riservatezza.

*Gli artt. 13, 14 e 15 della Costituzione*

Queste norme sanciscono l'inviolabilità della libertà personale, del domicilio, della libertà e segretezza della corrispondenza e ogni altra forma di comunicazione.

La libertà personale viene intesa non solo in senso fisico, ma con riguardo alla persona nella sua interezza, compresa la sfera spirituale e la sua personalità.

Parimenti, domicilio e corrispondenza sono interpretati come proiezione spaziale e spirituale dell'individuo.

*La maggior parte della dottrina esprime sfavore verso l'utilizzo di queste norme come ancora costituzionale per il diritto alla riservatezza.*

*L'art. 21 della Costituzione*

Questa norma è stata utilizzata per negare la rilevanza costituzionale del diritto alla riservatezza perché ritenuto incompatibile con la libertà di espressione; ma è stata anche utilizzata per

fondare il rango costituzionale del diritto alla riservatezza proprio su questa disposizione.

La giurisprudenza consolidata si fonda sul criterio di bilanciamento, relativo e non assoluto, ispirato ai tre parametri dell'*interesse sociale della notizia*, della *verità dei fatti narrati* e della *contingenza*.

*Fonti normative*

- Legge n. 675/1996
- L. D. n. 676/1996
- D. Lgs. n. 123/1997
- D. Lgs. n. 255/1997
- D. Lgs. n. 135/1998
- D. Lgs. n. 389/1998
- D. Lgs. n. 51/1999
- D. Lgs. n. 135/1999
- D. Lgs. n. 281/1999
- D. Lgs. n. 282/1999
- Legge n. 344/1998
- Legge n. 25/1999
- Legge n. 127/2001
- Legge n. 325/2000
- D. Lgs. n. 467/2001
- D.P.R. n. 318/1999
- D. Lgs. n. 196/2003
- Legge n. 45/2004

La legge fondamentale n. 675/1996 è stata più volte integrata e modificata fino al d. lgs. n. 196/2003 (Codice della privacy), a sua volta ancora integrato dalla legge n. 45/2004.

**IMPORTANTE DA RICORDARE**
La protezione dei dati personali: -non consiste nella copertura, ma nella loro "difesa".

## IL SIGNIFICATO DELLE ESPRESSIONI LETTERALI RICORRENTI NEL CODICE

**Trattamento**: è qualunque operazione o insieme di operazioni, compiute anche senza il supporto 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 sono registrati in una banca dati.

**Dato personale**: è qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificato o identificabili, anche in modo indiretto, mediante riferimento a qualsiasi altra informazione, compreso il numero di identificazione personale.
(Art. 2 Direttiva 95/46/CE "*qualsiasi informazione concernente una persona fisica identificata o identificabile; si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale*")

**Dati sensibili**: sono dati personali che permetto la rivelazione dell'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.

**Titolare**: 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 deci-

sioni relative alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza.

**Responsabile**: è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.

**Incaricati:** sono le persone fisiche autorizzate ad effettuare operazioni di trattamento dal titolare dei dati o dal responsabile.

**Interessato**: è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

**Comunicazione**: consiste nel portare a conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualsiasi forma, anche attraverso la loro messa a disposizione o consultazione.

**Diffusione**: consiste nel portare a conoscenza dei dati personali soggetti indeterminati, in qualunque forma, anche attraverso la loro messa a disposizione o consultazione.

**Blocco**: consiste nella conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

## *I DIRITTI DELL'INTERESSATO*
## *REGOLE GENERALI PER IL TRATTAMENTO DEI DATI*

Art. 7 Diritto di accesso ai dati personali e altri diritti

Art. 8 Esercizio dei diritti

Art. 9 Modalità di esercizio

Art. 10 Riscontro dell'interessato

Art. 11 Regole generali per il trattamento dei dati personali

- Leicità e correttezza
- Raccolta e registrazione per scopi determinati, espliciti e legittimi
- Esattezza
- Pertinenti, completi e non eccedenti rispetto alle finalità di utilizzo.
- Conversione finalizzata all'identificazione dell'interessato per il periodo necessario al raggiungimento dello scopo di raccolta e trattamento

Art. 12 Regole generali per il trattamento dei dati

Sono previsti codici deontologici e di buona condotta come fonti di norme flessibili e agevolmente modificabili.
Il rispetto delle disposizioni dei codici costituisce condizione essenziale per la laicità e correttezza del trattamento dei dati personali.

Regole generali per il trattamento dei dati

I codici trovano la loro radice in quelle "norme sulla normazione" costituite dagli articoli della direttiva-madre 95/46/CE.

La codificazione deontologica si pone come il punto di confluenza di tre fattori:

⇒ Atti comunitari;
⇒ Poteri propulsivi dell'autorità garante;
⇒ Elaborazione delle regole da parte dei soggetti professionali.

**Informativa:**

L'articolo 13 prevede i contenuti e i termini dell'informativa all'interessato o alla persona presso la quale sono raccolti i dati personali.

**Art. 15 (Danni cagionati per effetto del trattamento):**

1) Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.
2) Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

*Il richiamo all'art. 2050 del c.c. comporta l'inversione dell'onere della prova a carico di chi svolge attività pericolosa.*
*Pertanto chiunque provochi un danno ha l'obbligo di dimostrare di aver posto in essere ogni misura idonea ad evitarlo.*

**In caso di cessazione del trattamento i dati sono:**

⇒ distrutti;
⇒ ceduti ad altro titolare per un ulteriore trattamento compatibile con gli scopi originari della raccolta;
⇒ conservati per fini personali e sottratti a comunicazione o diffusione;
⇒ conservati o ceduti ad altro titolare a fini storici statistici o scientifici secondo le disposizioni normative.

**Articolo 17—Trattamento che presenta rischi specifici:**

1) Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.
2) Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

## *REGOLE ULTERIORI PER I SOGGETTI PUBBLICI*

Il Codice sulla Privacy investe responsabilità di soggetti PUBBLICI e PRIVATI.

Il Codice regola in modo specifico i caso in cui il trattamento avviene a cura di pubbliche amministrazioni.

1) 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.
2) Nei casi in cui una disposizione di **legge specifica la finalità di rilevante interesse pubblico**, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 15-4, comma 1, leggera g), anche su schemi tipo.
3) Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione della attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai seni dell'articolo 26, comma 2, il trattamento di dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.
4) L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

Tra le attività svolte dalla Pubblica Amministrazione il codice, per diversi comparti, precisa con molto dettaglio, le attività che investono “finalità di rilevante interesse pubblico”.

*La privacy e la trasparenza*
il Soggetto pubblico oltre all’esigenza di un controllo diffuso sui comportamenti amministrativi, ha la responsabilità di proteggere la riservatezza dai dati.

Il criterio della trasparenza amministrativa, va quindi bilanciato dal canone della protezione della riservatezza dei dati.

La normativa sui dati personale prevede che la conoscenza da parte di terzi di dati avviene attraverso una specifica forma di trattamento (comunicazione o diffusione) presupposta da un regolamento e/o da una norma di legge. Deve inoltre essere funzionale allo svolgimento dell’attività istituzionale, per la quale possono essere posti dei limiti da regolamenti o dalla normativa vigente.

La normativa sull’accesso ai dati riconosce la rilevanza della riservatezza come possibile limite all’estensibilità dei documenti amministrativi.

Nel bilanciamento tra i due interessi contrapposti Accesso/ riservatezza il cittadino conserva il diritto di visionare i documenti (quindi anche i dati sensibili) quanto vi è la motivata esigenza di far valere i propri diritti, non solo in sede giudiziaria.

Il criterio guida è la massima pubblicità e trasparenza da assicurare a tutti i soggetti legittimati secondo la Legge 241, osservando però alcune cautele:

⇒ Il bilanciamento tra interessi contrapposti è operato dal legislatore e confermato dai regolamenti sull’accesso in particolare ai dati sensibili;

⇒ Il diritto di accesso soccombe alla riservatezza. Tuttavia nel caso in cui il diritto di accesso venga esercitato su atti la cui conoscenza è necessaria per la cura o difesa di interessi giuridici, ma che contengono dati sensibili, il diritto di accesso va permesso nella forma della "visione".
⇒ I dati supersensibili (vita sessuale e salute) sono ostensibili solo quanto il richiedente, con istanza di accesso, intende tutelare una situazione giuridica di rango almeno pari al diritto dell'interessato, ovvero consistente in un diritto della personalità o un altro diritto o libertà fondamentale e inviolabile.

## LA PRIVACY NELL'ORDINAMENTO SCOLASTICO

Oltre alle fonti normative generali, troviamo i seguenti richiami normativi specifici:
⇒ art. 330 bis T.U. 297/94
⇒ art. 2, c. 2 D.P.R. 249/98 (regolamento sullo statuto delle studentesse e degli studenti).

I dati utilizzati e tratti dalla scuola concernono:
⇒ gli alunni e le rispettive famiglie
⇒ il personale scolastico
⇒ altri soggetti relativamente ad attività svolte nella scuola o nell'esercizio dell'azione amministrativa.

La scuola svolge la sua attività in ambito istituzionale e nel ruolo di datore di lavoro.

*ATTIVITÀ ISTITUZIONALE*

Nell'ambito delle attività istituzionali il codice consente il trattamento di dati personali "solo per lo svolgimento delle funzioni istituzionali" (art. 18 comma 2) e la comunicazione e diffusione

"… unicamente quando sono previste da una norma di legge o regolamento" (u.c. art. 19).
In questi casi i soggetti pubblici non devono richiedere il consenso all'interessato.

La scuola svolge attività istituzionale:

⇒ per attività amministrative strumentali (art. 1 della Legge 53/2003): "Al fine di favorire la crescita e la valorizzazione della persona umana, nel rispetto dei ritmi dell'età evolutiva, delle differenze e dell'identità di ciascuno e delle scelte educative della famiglia, nel quadro della cooperazione tra scuola e genitori, in coerenza con il principio di autonomia delle istituzioni scolastiche e secondo i principi sanciti dalla Costituzione …" ;

⇒ nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti (art. 18, 3° comma cod.);

⇒ Il trattamento è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente (art. 19 cod.).

L'art. 19 del codice sulla privacy prevede tre casi (per i soli dati personali):

⇒ il trattamento dei dati personali da parte di soggetti pubblici: possibile per lo svolgimento delle funzioni istituzionali;

⇒ la comunicazione di dati personali da parte di soggetti pubblici ad altri soggetti pubblici: possibile se prevista da norme di legge o Regolamenti o sono necessarie per lo svolgimento di funzioni istituzionali nel rispetto dell'art. 39;

⇒ la comunicazione di dati personali da parte di soggetti pubblici e privati e la diffusione di tali dati: possibile solo se previste da norme di Legge o regolamenti.

L'art. 39 prevede l'obbligo di comunicazione.

Il titolare del trattamento p tenuto a comunicare previamente al Garante la comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione.

Al momento della racconta dei dati personali da parte dell'istituzione scolastica, l'interessato, ai sensi dell'art. 13 deve essere informato:

⇒ sulle finalità e modalità di trattamento dei dati;
⇒ sulla natura obbligatoria o facoltativa del conferimento;
⇒ sulle conseguenze di un eventuale rifiuto a rispondere;
⇒ sui soggetti ai quali i dati possono essere comunicati;
⇒ sui diritti ex art. 7 ;
⇒ sul titolare ed il responsabile del trattamento.

Come si è già precedentemente evidenziato, l'informativa è esclusa quando i dati sono trattati in base ad un obbligo di legge o regolamento o normativa comunitaria.

Se i dati sono "sensibili" vanno applicati gli artt. 20 e 22, 95 e 96.

Art. 20, c. 1
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.

L'art. 22 elenca ulteriori principi applicabili al trattamento dei dati sensibili e giudiziari. In questo articolo sono confluiti in modo ordinario e coordinato i precetti contenuti nei decreti integrativi della legge n. 675/1996, in particolare le disposizioni sul trattamento dei dati sensibili contenuti nel D. Lgs n. 135/1999.

Il principio di minimizzazione del trattamento prevede nella trattazione dei dati sensibili con strumenti informatici:

⇒ la copertura cifrata
⇒ tutela da estranei ma anche da chi è autorizzato all'accesso;
⇒ identificazione solo in caso di necessità.

L'art. 22 dedica una particolare attenzione ai dati sensibili idonei a rivelare lo stato di salute e la vita sessuale, prevedendo ulteriori cautele rispetto a quelle generali.
Il comma 7 prevede che essi devono essere conservati separatamente da altri dati personali e che non possano essere diffusi.

L'art. 20: prevede il trattamento dei dati "sensibili" solo se riconosciute le finalità di interesse pubblico.

L'art. 95: qualifica "di interesse pubblico" le finalità di istruzione e di formazione.

L'art. 96: regolamenta il trattamento dei dati relativi agli studenti.

L'art. 95 (dati sensibili e giudiziari) considera di rilevante interesse pubblico, ai sensi degli artt. 20 e 21, le finalità di Istruzione e formazione in ambito scolastico, professionale o universitario, con particolare riferimento a quelle svolte anche in forma integrata.

Manca in ogni caso l'"**espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili".**

Dunque il trattamento è consentito solo per i dati identificati e resi pubblici dal titolare dei trattamenti, in relazione alle specifiche finalità perseguite nei singoli casi, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante

(art. 20).

In questo caso i soggetti pubblici possono richiedere al Garante l'individuazione delle attività che perseguono finalità di interesse pubblico

*ATTIVITÀ SVOLTE NEL RUOLO DI DATORE DI LAVORO*

L'art. 112 insiste sulla nozione delle finalità di rilevante interesse pubblico e consente di rilevare analiticamente le varie attività nelle quali è ammesso il trattamento dei dati personali per l'instaurazione e la gestione dei rapporti di lavoro, e inoltre i limiti imposti alla diffusione e comunicazione dei dati stessi.

Ai sensi del combinato disposto degli artt. 112, 20 e 21 del codice, la disciplina del trattamento dei dati sensibili e giudiziari sarà vincolata alla predisposizione da parte dei soggetti pubblici interessati all'emanazione di un "atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'art. 154, comma 1, lettera g) anche su schemi tipo".

Ciò nel caso in cui la legge specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il cambiamento.

L'art. 112 elenca finalità direttamente o indirettamente connesse al rapporto di lavoro in tutte le sue fasi.
Al comma 2 inoltre, elenca finalità che non sono direttamente ricollegabili alle fasi evolutive del rapporto di lavoro (lettera f)
Infine sono elencate finalità di rilevante interesse pubblico riconducibili laut sensu al lavoro pubblico (es. lettere g e h).

Obiettivo degli adempimenti previsti dall'art. 31 è la riduzione al minimo di determinati rischi.

Il Codice dispone innanzitutto che i dati personali oggetto di trattamento siano custoditi e controllati. Gli obblighi sono quindi:

⇒ la custodia: che presuppone, in genere, l'allocazione dei dati in modo tale da garantirne la permanenza e l'integrità;

⇒ il controllo: che implica un'attività da parte del preposto finalizzata alla verifica della permanenza delle condizioni del dato.

Questi obblighi vanno declinati in relazione:

⇒ alle conoscenze acquisite in base al progresso tecnico: pertanto con l'uso di strumenti di sicurezza sia meccanica, che elettronica, che informatica;

⇒ alla natura dei dati: la distinzione riguarda i dati personali e i dati sensibili;

⇒ alle specifiche caratteristiche del trattamento: la casistica comprende tutte le accezione di trattamento elencate nell'-art. 4, lett. A) del Codice, vale a dire 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 dati.

Gli obblighi appena esaminati nell'art. 31 rappresentano solo una parte degli accorgimenti obbligatori in materia di sicurezza, poiché, nell'ambito del predetto obbligo generale, vi è il dovere di adottare in ogni caso le "misure minime" (art. 33).

In aggiunta alle conseguenze previste per la violazione degli obblighi di cui all'art. 31, il Codice prevede che l'omessa adozione delle misure minime, secondo le modalità contenute nell'-allegato B del Codice, concretizzi anche un reato, così come

previsto dall'art. 169 del Codice.

*Art. 169. Misure di sicurezza*
*1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni [o con l'ammenda da diecimila euro a cinquantamila euro].*
*2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al [quarto del massimo dell'ammenda stabilita per la contravvenzione] quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.*

Come già previsto in passato, le misure minime da adottare sono diverse a seconda che il trattamento sia effettuato con strumenti elettronici o meno, oppure riguardi dati sensibili o giudiziari. L'art. 180 del Codice prevede che le nuove misure, di cui agli articoli 33-35 del Codice, e l'Allegato B, non previste dal D.P.R. n. 318/99, sono adottate entro il 30 giugno 2004, termine prorogato al 30 giugno 2005 (art. 34).

In ogni caso occorre:
- ⇒ nominare le figure previste dal codice (titolare, incaricati);
- ⇒ attivare un cluster di password con particolari caratteristiche;

⇒ adottare programmi al fine di prevenire la vulnerabilità degli strumenti elettronici, aggiornandoli annualmente;
⇒ salvare i dati almeno ogni settimana;
⇒ Redigere il Documento programmatico sulla sicurezza.

L'Allegato B disciplina in un apposito Titolo, le modalità di trattamento di dati senza l'ausilio di strumenti elettronici. La lett. C) riguarda al punto 29 laddove è previsto che l'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Vanno identificati i soggetti che chiedono di accedere e qualora non vi siano strumentazioni elettroniche di controllo, è necessaria una specifica autorizzazione (art. 35).

*IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA INFORMATICA*

È stato confermato il principio secondo cui le "misure minime", di importanza tale da indurre il legislatore a prevedere anche una sanzione penale, sono solo una parte degli accorgimenti obbligatori in materia di sicurezza:

Si distinguono due obblighi:
⇒ l'obbligo più generale di ridurre al minimo determinati rischi;
⇒ nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le "misure minime".

Il Codice prevede l'adozione di alcune misure indispensabili, dette minime, le cui modalità sono specificate tassativamente nell'allegato B del Codice.

**Il documento programmatico sulla sicurezza** è una delle misure minime e deve essere adottato dal titolare di un trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici, attraverso l'organo, l'ufficio o persona fisica a ciò legittimata in base all'ordinamento aziendale o della pubblica amministrazio-

ne interessata.

**La Relazione accompagnatoria al bilancio d'esercizio**, rappresenta anch'essa una misura minima. Il Codice ha introdotto questa nuova regola per rendere edotti gli organi di vertice del titolare del trattamento e responsabilizzarli in materia di sicurezza, attraverso l'obbligo di riferire nella relazione di accompagnamento di ciascun bilancio di esercizio circa l'avvenuta redazione o aggiornamento del DPS.

*STRUTTURA DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA*

L'elenco dei trattamenti di dati personali di si divide in:
⇒ informazioni essenziali
⇒ ulteriori elementi descrittivi

Le informazioni essenziali prevedono:
⇒ la descrizione sintetica del trattamento;
⇒ la finalità perseguita o l'attività svolta;
⇒ le categorie di interessati;
⇒ la natura dei dati;
⇒ la struttura di riferimento;
⇒ eventuali altre strutture che concorrono al trattamento;
⇒ descrizione degli strumenti utilizzati.

Gli ulteriori elementi descrittivi da indicare facoltativamente sono:
⇒ l'identificativo del trattamento;
⇒ eventuale banca dati;
⇒ ubicazione fisica dei supporti di memorizzazione;
⇒ tipologia di dispositivi di accesso;
⇒ tipologia di interconnessione.

Nella struttura del DPS è prevista la distribuzione dei compiti e delle responsabilità. In questa sezione vanno descritti sintetica-

mente l'organizzazione della struttura di riferimento, i compiti e le connesse responsabilità, in relazione ai trattamenti effettuati. Possono essere richiamati documenti già prodotti indicandone le modalità di reperimento.

L'analisi dei rischi che incombono sui dati è prevista quale descrizione di eventi potenzialmente dannosi per la sicurezza dei dati, con la relativa valutazione delle possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

Nella sezione delle misure in essere e da adottare, vanno riportate sinteticamente le misure già praticate e da adottare per contrastare i rischi individuati.
Per misura si intende lo specifico intervento tecnico ed organizzativo realizzato e le attività di monitoraggio e controllo essenziali per assicurarne l'efficacia. Riassumendo:

⇒ **Misure**: descrivere sinteticamente le misure adottate (seguendo anche le indicazioni contenute nelle altre regole dell'Allegato B del Codice);

⇒ **Descrizione dei rischi**: per ciascuna misura indicare sinteticamente i rischi che si intende contrastare (anche qui, si possono utilizzare le indicazioni fornite dall'Allegato B);

⇒ **Trattamenti interessati**: indicare i trattamenti interessati per ciascuna delle misure adottate;

⇒ Determinate misure possono non essere riconducibili a specifici trattamenti o banche di dati (ad esempio, con riferimento alle misure per la protezione delle aree e dei locali);

⇒ Occorre specificare se la misura è già in essere o da adot-

tare, con eventuale indicazione, in tale ultimo caso, dei tempi previsti per la sua messa in opera.

⇒ **Struttura o persone addette all'adozione**: indicare la struttura o la persona responsabile o preposta all'adozione delle misure indicate.

Nella sezione dei criteri e modalità di ripristino delle disponibilità dei dati, vanno descritte le procedure adottate per il ripristino dei dati in caso di un loro danneggiamento. È quindi necessario che le copie dei dati siano disponibili e le procedure di re installazione efficaci.

Per quanto riguarda il ripristino dei dati le informazioni essenziali sono:

⇒ Banca dati/Data base/Archivio: indicare la banca dati, il data base o l'archivio interessati;
⇒ Criteri e procedure per il salvataggio e il ripristino dei dati: descrivere sinteticamente le procedure, la tipologia di salvataggio e la frequenza con cui viene effettuato;
⇒ Modalità di custodia delle copie: indicare il luogo fisico in cui sono custodite le copie dei dati salvate;
⇒ Struttura o persona incaricata del salvataggio: indicare la struttura o le persone incaricate di effettuare il salvataggio e/o di controllarne l'esito;
⇒ Il criteri individuati per il salvataggio e il ripristino dei dati, con eventuale rinvio ad un'ulteriore scheda o a documentazioni analoghe;
⇒ Pianificazione delle prove di ripristino: indicare i tempi previsti per effettuare i test di efficacia delle procedure di salvataggio/ripristino dei dati adottate.

Nella sezione riguardante la pianificazione degli interventi formativi, si descrive il piano formativo che si intende attuare. In particolare si descrivono sinteticamente gli obbiettivi e le moda-

lità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 (ingresso in servizio o cambiamento di mansioni degli incaricati, introduzione di nuovi elaborati, programmi o sistemi informatici, etc.).

Vengono altresì indicate le classi di incarico a cui è destinato l'intervento formativo e le tipologie di incaricati interessati, anche in riferimento alle strutture di appartenenza.

Vanno inoltre indicati i tempi previsti per lo svolgimento degli interventi formativi.

Nella sezione sui trattamenti di dati affidati all'esterno, deve essere redatto un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, indicando sinteticamente il quadro giuridico o contrattuale in cui tale trasferimento si inserisce, relativamente agli impegni assunti anche all'esterno, per garantire la protezione dei dati.

A tal fine vanno riportate le seguenti informazioni essenziali:

⇒ descrizione dell'attività esternalizzata: indicare sinteticamente l'attività affidata all'esterno;

⇒ trattamenti di dati interessati: indicare i trattamenti di dati, sensibili o giudiziari, effettuati nell'ambito della predetta attività;

⇒ soggetto esterno: indicare la società, l'ente o il consulente cui è stata affidata l'attività e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento);

⇒ Descrizione dei criteri: perché sia garantito un adeguato trattamento dei dati è necessario che la società a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento, ad esempio a:

1) trattamento di dati ai soli fini dell'espletamento dell'in-

carico ricevuto;
2) adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
3) rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
4) impegno a relazionare periodicamente sulle misure di sicurezza adottate—anche mediante eventuali questionari e liste di controllo—e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenza.

Per quanto concerne la cifratura dei dati o separazione dei dati identificativi, tale operazione riguarda esclusivamente gli operatori sanitari, poiché concerne le modalità di protezione adottate in relazione ai dati per cui è richiesta cifratura o la separazione fra dati identificativi e dati sensibili, oltre ai criteri per assicurare la sicurezza di tali trattamenti.

## ALCUNI CASI SCOLASTICI

Di seguito si offrono alcuni chiarimenti su casistiche specifiche della scuola in ordine all'applicazione del Codice sulla Privacy:

LE CIRCOLARI
Le circolari scolastiche devono rispettare le leggi sulla privacy e non possono contenere dati personali che consentano di risalire, anche se in modo indiretto, all'identità di studenti qualora le informazioni ledano la loro riservatezza.

I QUADRI
Rendere noti nominativamente i risultati scolastici, anche negativi, non costituisce violazione della privacy, poiché la pubblicità in questa materia è obbligo e regola generale.

Sussistono infatti esigenze di controllo sociale e professionale che dipendono proprio dalla conoscibilità delle valutazioni finali.

CORSI PARTICOLARI
Nel caso di comunicazioni relative a corsi particolari il Garante ha rilevato che tali informazioni potrebbero essere inerenti e quindi rilevare lo stato di salute dei soggetti interessati, per cui rientrerebbero nei “dati sensibili”.

RIPRESE VIDEO E FOTOGRAFIE RACCOLTE DAI GENITORI DURANTE RECITE E SAGGI SCOLASTICI
Il Garante ha rilevato che l’uso di videocamere o macchine fotografiche per documentare eventi scolastici e conservare ricordi dei propri figli non rientra nel concetto di privacy, poiché si tratta di immagini raccolte per fini personali, il cui uso è del tutto legittimo.

DATI SUL SITO WEB DI UNA SCUOLA
I dati presenti sul sito web curato da una scuola e riferiti ad alunni disabili concretizzano un trattamento illegittimo, per cui il Garante non ha consentito la prosecuzione.

DATI CHE RIGUARDANO IL LAVORATORE
Vige il principio della tenuta separata dei dati sensibili da quelli ordinari, in modo da garantire cautela e accorgimenti nella consultazione ordinaria.

CEDOLINI DELLO STIPENDIO
Nel cedolino vanno riportate le notizie indispensabili al lavoratore per ricostruire le fonti di entrata, ma non vanno indicate causali specifiche di trattenute, né la denominazione del sindacato a favore del quale è versata la ritenuta sindacale.

PROCEDURE DI CONCILIAZIONE OBBLIGATORIA
Non è ammessa la comunicazione a soggetti non coinvolti nella

procedura, trattandosi di comunicazione illecita, perché effettuata in mancanza di una specifica disposizione di legge e di regolamento che la consenta.

FONDO DI ISTITUTO

La ripartizione del fondo può essere affissa all'albo rientrando nelle previsioni dell'art. 112 del Codice in tema di adempimenti concernenti obblighi retribuitivi.