D. Lgs.196/2003

Codice in materia di protezione dei dati personali

(Privacy)

Presentazione

per

Assistenti Amministrativi

art. 33 – D.Lgs. 196/03 - Misure minime

- Nel quadro dei più generali obblighi di sicurezza di cui all'art.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'art. 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati

Documento programmatico sulla sicurezza

(da redigere entro il 31 marzo di ogni anno)

Contenuti

19.1 - elenco dei trattamenti di dati personali

19.2 - distribuzione dei compiti e delle responsabilità (incarichi scritti)

19.3 - analisi dei rischi che incombono sui dati

19.4 - misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione dei locali

19.5 - descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

19.6 - previsione di interventi formativi degli incaricati del trattamento

La formazione del personale relativamente ai temi qui trattati

- Il Codice della privacy rende obbligatoria la formazione del personale e nel Documento Programmatico sulla Sicurezza è obbligatorio indicare il *programma* di formazione.

Gli Assistenti Amministrativi possono/devono essere nominati "incaricati del trattamento" ? (eterointegrazione del contratto)

- Questo non comporta attività supplementari rispetto a quelle già svolte (come nei casi dei "Collaboratori" o degli incarichi retribuiti) , ma semplicemente l'autorizzazione a trattare certi dati e la prescrizione delle cautele da osservare.

RESPONSABILITÀ CIVILISTICA - Art. 2050 C.C.
Ricorso al giudice civile

- Art. 15 impone il dovere di risarcire (ai sensi dell'art. 2050 del Codice Civile) i danni causati ad altri per effetto del trattamento di dati personali o per la violazione delle regole di trattamento.
- Art. 2050 C.C. "Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee ad evitare il danno".
- A causa di questa specifica disposizione *esiste l'inversione dell'onere della prova e c'è una presunzione di colpevolezza automatica da parte del Titolare.*
- Ci si libera da tale presunzione di colpevolezza, dimostrando con prove concrete di aver preso tutte le misure idonee e le cautele per prevenire il danno.

Protezione dei dati personali

Art. 4 – D.Lgs.196/03

Ai fini del presente codice si intende per:

a) "trattamento" qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la:

- raccolta
- registrazione
- organizzazione
- conservazione
- consultazione
- elaborazione
- modificazione
- selezione
- estrazione
- raffronto
- utilizzo
- interconnessione
- blocco
- comunicazione, diffusione, cancellazione, distruzione di dati
- nonché il semplice possesso dei dati anche se non registrati in una banca dati

Art. 4 – D.Lgs.196/03

b) "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.

art. 4 – D.Lgs.196/03

c) "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
- l'adesione a sindacati
- l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- lo stato di salute
- la vita sessuale

La definizione di dato sensibile è esclusiva (solo quelli indicati).

art. 4 – D.Lgs.196/03

d) "dati giudiziari" i dati personali idonei a rivelare provvedimenti in materia di:

- iscrizione nel casellario giudiziale
- iscrizione nell'anagrafe delle sanzioni amministrative dipendenti da reato
- avere carichi pendenti
- avere la qualità di imputato o indagato

art. 17 – D.Lgs.196/03

e) "dati particolari" dati diversi da quelli sensibili e giudiziari che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

esempio: provvedimenti disciplinari

» dati patrimoniali

» particolari immagini, foto o video

art. 4 – D.Lgs.196/03

"Comunicazione"

- il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

"Diffusione"

- il dare conoscenza dei dati personali a soggetti indeterminati in qualunque forma, anche mediante la loro messa a disposizione o consultazione (albo della scuola, internet)

"Interessato"

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

Diritti dell'Interessato (art. 7 – 10)

- L'Interessato (persona o ente o associazione) ha il diritto di conoscere i dati che lo riguardano e in certi casi di intervenire su di essi per farli cancellare, modificare o aggiornare. Detti diritti vanno illustrati per esteso nell'informativa.
- Da notare che si tratta di cosa diversa dal diritto di accesso ai documenti amministrativi sancito dalla legge 241 (vedi artt. 59 e 60).

Informativa all'Interessato (Art. 13)

L'Interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati

b) la natura obbligatoria o facoltativa del conferimento dei dati

c) le conseguenze di un eventuale rifiuto di rispondere

d) 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 dati medesimi

Informativa all'Interessato (Art. 13)

- Va sottolineato che mentre per l'interessato (o chi lo rappresenta nel caso di minore) fornire certi dati è un obbligo per ottenere il servizio scolastico, in altri casi invece ciò è facoltativo ed eventualmente comporta soltanto la perdita di una qualità ulteriore del servizio. Ciò deve essere esplicitato nell'informativa.
- Se i dati personali non sono raccolti presso l'interessato, l'informativa deve essere data al medesimo Interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, gli vanno anche specificate le categorie di dati trattati.

Art. 22 - Principi applicabili al trattamento di dati sensibili e giudiziari

Nel fornire l'informativa di cui all'articolo 13, i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati comuni, sensibili, giudiziari e particolari.

art. 28 – D.Lgs. 196/03

"titolare del trattamento" la pubblica amministrazione cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Nel caso della scuola il Dirigente Scolastico.

art. 29 – D.Lgs.196/03

- Il "responsabile del trattamento" è designato dal titolare al trattamento dei dati personali e procede alla nomina degli incaricati, alla formazione degli stessi, nonché in accordo con il titolare all'adozione di tutte le misure idonee a garantire la sicurezza dei dati trattati.
- D.S.G.A e/o altro dipendente.

art. 30 – D.Lgs.196/03

"Incaricati del trattamento"

Riguarda tutto il personale della scuola

- le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile.
- La designazione è effettuata per iscritto (nomina) e individua puntualmente l'ambito del trattamento consentito.

art. 18 – D.Lgs.196/03 Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici
(esclusi quelli economici)

- C.2. Qualunque trattamento di dati personali da parte di enti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

  (Principio di necessità e Principio di finalità istituzionale)

- C.4. … i soggetti pubblici *non devono richiedere* il consenso all'interessato.

  Ove prevista, l'acquisizione del consenso dell'interessato non legittima in nessun caso l'ente pubblico a trattare dati personali per finalità diverse da quelle istituzionali.

Trattamento di dati non sensibili e dati non giudiziari

I soggetti pubblici:

a) Hanno a priori l'autorizzazione al trattamento di tutti quei dati che non siano sensibili né giudiziari (purchè siano strettamente necessari all'attività istituzionale).

b) Sono esentati dall'obbligo di richiedere il consenso dell'Interessato, però non sono esentati dall'informativa.

c) Hanno diritto a comunicare dati (ma non quelli sensibili o giudiziari) ad altri enti pubblici a condizione che tale comunicazione sia espressamente prevista da una legge o regolamento.

d) Hanno diritto a diffondere dati (ma non quelli sensibili o giudiziari) esclusivamente a condizione che sia espressamente previsto da una legge o regolamento (Tabellone con i voti degli scrutini).

art. 35 – D.Lgs.196/03 - Trattamenti senza l'ausilio di strumenti elettronici

Misure minime per i trattamenti cartacei

- Aggiornamento periodico dell'ambito del trattamento consentito
- Lista degli incaricati
- Istruzioni scritte agli incaricati per custodia e controllo
- Idonea custodia di atti e documenti
- Controllo e custodia fino alla restituzione
- Accesso agli atti alle sole persone autorizzate
- Accesso agli archivi controllato

CAPO II - ILLECITI PENALI

Art. 167. Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

TITOLO III - SANZIONI
CAPO I - VIOLAZIONI AMMINISTRATIVE

Art. 161 - Omessa o inidonea informativa all'interessato

La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da *tremila euro a diciottomila euro* o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, *da cinquemila euro a trentamila euro*. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

Istruzioni generali

Sarebbe necessario che ogni volta che la Segreteria raccoglie o tratta un nuovo dato sensibile o giudiziario:

- prima di tutto lo individuasse come tale ,
- subito dopo trovasse le norme legislative in base a cui quello specifico dato è richiesto o trattato,
- infine procedesse a informare di questo l'interessato, costituendo la prova della predetta informativa prima di cominciare qualsiasi trattamento.

Disposizioni

Delega per la riscossione delle quote sindacali

L' eventuale scelta del sindacato a favore del quale viene rilasciata delega per la riscossione delle relative quote è da annoverare tra i dati sensibili; pertanto la riservatezza della stessa dovrà essere in ogni caso assicurata.

Dati sensibili presenti nei fascicoli dei dipendenti

I dati sensibili contenuti nei fascicoli personali dei dipendenti devono essere conservati *separatamente* rispetto alle altre informazioni negli stessi contenute.

Cartelle sanitarie e di rischio (art. 17, comma 1, D.Lgs n.626/94)

La massima accortezza dovrà essere adottata anche nei riguardi delle cartelle sanitarie e di rischio relative ai lavoratori sottoposti a sorveglianza, redatte ed aggiornate dal medico competente, della cui custodia è peraltro responsabile l'Istituto, quale datore di lavoro.

Classificazione dati

Non appena un Incaricato si accorge che un documento contiene dati personali di livello superiore a "comune" o "anonimo" scriva in matita sull'angolo destro superiore del foglio:

- una prima lettera descrivente il tipo di dato
"P"= dato particolare
"S"= dato sensibile
"**G"=** dato giudiziario (nel dubbio va scelto il livello superiore)

seguita da una seconda lettera che gradua il livello di riservatezza all'interno della categoria assegnata

"B" (=basso) se si tratta di dato che per la sua natura rivela un'informazione modesta e poco pericolosa per l'Interessato se conosciuta da estranei (es. certificato medico generico privo di diagnosi e di qualsiasi riferimento alla malattia o infortunio che lo ha generato e con prognosi di pochi giorni

"A" (=alto) per tutti gli altri casi. Nel dubbio, va scelta la lettera "A".

Naturalmente, se l'Incaricato ha dei dubbi per la classificazione, deve rivolgersi al Responsabile o al Titolare.

L’informativa per i dati che ci pervengono tramite posta o posta elettronica

- Nei casi in cui un dato personale di una persona che non abbia avuto precedenti rapporti con la scuola, ci perviene saltando lo sportello, prima di cominciare a trattare i dati personali dell’Interessato, si dovrebbe dargli l’informativa.
- La soluzione può essere di avvertire telefonicamente che il trattamento non potrà cominciare fino a che non si presenta allo sportello, oppure mandare l’informativa per posta o per e-mail (cosa di cui è possibile mantenere copia come prova).

Certificati Medici

- I certificati medici prodotti senza la diagnosi e in cui risulta soltanto la prognosi, tecnicamente sono ancora ascrivibili ai dati sensibili, tuttavia è evidente che in realtà forniscono un'informazione assai modesta sullo stato di salute (tuttavia se la prognosi fosse di molti mesi, già ci sarebbe sentore di un problema grave di salute).
- Anche il banale certificato medico che supporta la richiesta di esonero da educazione fisica sulla base di una diagnosi di distorsione della caviglia, tecnicamente è un dato sensibile, ma nella realtà è scarsamente significativo.
- Qualcuno sostiene, non senza fondamento, che anche la registrazione delle assenze per malattia, essendo idonea a rivelare lo stato di salute, sia un dato sensibile.
- Invece, probabilmente, il certificato di sana e robusta costituzione, se non evidenzia problematiche di salute, è solo un dato "particolare".

Insegnamento Religione Cattolica (dato sensibile)

L'adesione all'insegnamento della Religione Cattolica può essere considerato un dato sensibile perché rivela con ottimo grado di probabilità la convinzione religiosa della famiglia e/o dell'Interessato.

OTTO PER MILLE (dato sensibile.)

Invece la scelta della devoluzione dell'otto per mille segnata sul modulo Irpef è considerata sicuramente dato sensibile.

Rilevazioni delle presenze sul posto di lavoro e diritto di accesso ai dati

(Comunicato stampa del GARANTE)
Anche le rilevazioni effettuate mediante "badge" magnetico e conservate in un archivio informatico costituiscono dati personali e possono essere oggetto di una richiesta di accesso.

Procedura di Protezione Dati **PP13:** quando un alunno o un dipendente ci lascia definitivamente

- Gli vanno consegnati tutti i documenti contenenti dati personali che la scuola non sia obbligata a conservare.
  Nel caso non fosse possibile trattare direttamente con l'Interessato, si deve mandare un avviso per il ritiro.
  Nel frattempo i materiali da consegnare vanno posti in busta chiusa.
  Al ritiro va fatta firmare una ricevuta.
  Se passato un lasso ragionevole di tempo, l'interessato o un suo delegato non si presenterà a ritirarli, si avvierà una procedura di distruzione dei documenti, con apposito verbalino, ovviamente valutando prima se ci sono documenti che non sia opportuno eliminare (ad esempio, diplomi originali e simili).
- In ogni caso qualunque fascicolo personale che transiti dall'archivio corrente a quello storico, dev'essere prima depurato di tutti dati personali non più necessari.

Procedura di Protezione Dati **PP17**: trattamento appena un documento viene ricevuto

- L'Incaricato che riceve "brevi manu" allo sportello o in qualsiasi altro punto della scuola documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza ancora non collocati in busta chiusa, deve immediatamente metterli in busta chiusa e inserirli nella posta in arrivo per il Dirigente Scolastico.

Procedura di Protezione Dati **PP25** : Regole generali per la sicurezza degli archivi

- Ogni stanza-archivio deve essere chiusa a chiave quando non presenziata, anche se i documenti sono custoditi in contenitori chiusi a chiave, in quanto aumenta il livello di protezione dei dati stessi.

Procedura di Protezione Dati **PP27**: Archiviazione separata

I documenti contenenti dati sensibili, giudiziari o particolari ad alto livello di delicatezza vanno di norma chiusi in busta di carta, su cui è riportato nome dell'interessato, tipo di documento, data attuale e la scadenza per la eliminazione (se non conoscibile, mettere una data presunta seguita da un punto interrogativo). Per i documenti contenenti dati particolarmente sensibili, invece del nome sulla busta si deve scrivere un codice, la data attuale e la scadenza per la eliminazione.

La corrispondenza tra codice e nome dell'interessato sarà riportata in un foglio o un quaderno, posto in una busta chiusa gestita dal Responsabile o dal Titolare, e posto in luogo sicurissimo e protetto.

La busta viene archiviata in uno degli Armadi cosiddetti "dei Dati Protetti" (permanentemente chiuso a chiave, ad accesso controllato, in una stanza normalmente chiusa a chiave quando non presenziata[e protetta da antifurto]).

Al posto del documento così protetto viene messo nel fascicolo un foglio con annotazione generica del tipo di documento, della sua collocazione e della scadenza di distruzione.

Procedura di Protezione Dati **PP31** : archiviazione nel fascicolo personale

- I documenti non archiviati nell'Armadio di Protezione dati, finché l'alunno è iscritto o il dipendente è in servizio, vengono conservati nel fascicolo personale. In particolare alcuni dati si situano in una zona di confine tra dato particolare e dato sensibile (ad es. certificati medici generici privi di diagnosi), data la loro bassa pericolosità vengono mantenuti nel fascicolo personale, ma in una cartella separata, fino a fine anno scolastico, poi eliminati con la procedura di Protezione Dati **PP37**. Il fascicolo personale è conservato nel relativo archivio corrente: in cassettiere metalliche chiuse a chiave negli orari non lavorativi e normalmente presidiate da almeno un Incaricato dei trattamenti (ovvero un dipendente assegnato alla segreteria), in una stanza in cui non sono ammessi di regola estranei, che viene chiusa a chiave al di fuori dell'orario lavorativo.

Procedura di Protezione Dati **PP35** : scarto periodico dei documenti

- Scarto periodico dei documenti contenenti dati personali di qualunque livello , ai sensi dell'art. 11 comma e del D.Lgs 196/2003, vanno eliminati non appena cessa lo scopo per cui sono stati raccolti. Pertanto periodicamente, all'inizio di ogni anno solare per le pratiche che hanno questa cadenza, oppure all'inizio di ogni nuovo anno scolastico tutti gli archivi vengono passati al vaglio e vengono eliminati i documenti non più necessari, utilizzando la Procedura di promezione Dati **PP37**

Procedura di Protezione Dati **PP41** : cautele nella fase di fotocopiatura

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere fotocopiati, hanno la precedenza su tutti gli altri e devono essere adottate opportune cautele affinché nessun altro ne possa prendere visione. Tranne impossibilità tecnica, l'operazione di fotocopiatura deve essere effettuata dall'Incaricato che tratta la pratica. L'Incaricato deve fare in modo che il documento non venga lasciato in giacenza vicino alla fotocopiatrice né prima né dopo la fotocopiatura. A maggior ragione questo si applica se l'operazione di fotocopiatura avviene in una stanza ad accesso libero.

Procedura di Protezione Dati **PP43**: la movimentazione da parte di terzi

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere movimentati attraverso Collaboratori scolastici Incaricati, anche all'interno della scuola, devono essere collocati in busta chiusa. Anche la spedizione postale o la consegna in altro modo deve essere effettuata esclusivamente da Incaricati che abbiano ricevuto almeno l'autorizzazione a questo ambito di trattamento e che assicurino massima diligenza nella custodia dei plichi.

Procedura di Protezione Dati **PP45**: pulizia dei locali contenenti archivi

L’accesso di dipendenti o estranei per la pulizia dei locali contenenti archivi cartacei deve essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni, peraltro brevi, devono essere effettuate in presenza di un Incaricato della segreteria. Se vi sono contenuti dati sensibili sono chiudibili in contenitore, la pulizia deve essere effettuata esclusivamente alla presenza di un Incaricato del trattamento di tali dati.

Procedura di Protezione Dati **PP49**: ingresso di altre persone in segreteria

- Di norma l'ingresso in segreteria, nelle ore lavorative, è riservato a chi vi lavora, al Dirigente e ai suoi collaboratori, ai Collaboratori scolastici che ne hanno motivo. Gli altri dipendenti e gli estranei di norma non possono accedere, salvo che ne facciano richiesta preventiva e ne ottengano l'autorizzazione di volta in volta.
- Ciò viene previsto allo scopo di evitare che persone non autorizzate vedano anche involontariamente documenti riservati, è cautelativa la password su screen saver.
- La segreteria deve essere chiusa a chiave quando non è presenziata da chi vi lavora. Possibilmente le pulizie devono essere organizzate in orari in cui vi sia almeno un Assistente Amministrativo presente.

Procedura di Protezione Dati **PP61**: uso dei supporti rimovibili

- I floppy disk, le pen drive e i CD non devono essere utilizzati mai per memorizzare i file contenenti dati personali; tali files vanno invece memorizzati solo nel disco fisso di computers protetti da sistema di credenziali di accesso. Ciò al fine di evitare che chi si impadronisca di tali supporti rimovibili, possa accedere ai dati.
  I supporti rimovibili (floppy disk, pen drive e i CD) devono essere utilizzati esclusivamente per le copie di sicurezza (back-up) e subito devono essere riposti nel luogo sicuro indicato.

Procedura di Protezione Dati **PP63**: cautele nel riutilizzo dei supporti rimovibili

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (= formattando il disco e verificando l'avvenuta riformattazione; non basta assolutamente cancellare i files !)

Procedura di Protezione Dati **PP07**: firma l'Interessato o c'è sua delega scritta

- Qualunque trattamento di dati su richiesta dell'Interessato, se presentato da terzi dev'essere tassativamente autorizzato da delega. Ovviamente per gli alunni minorenni, il genitore o la persona esercente la patria potestà non ha bisogno di delega. *Per gli alunni maggiorenni anche il genitore ha bisogno della delega*.
- La delega va allegata all'informativa o all'istanza o alla ricevuta.

Art. 112 Finalità di rilevante interesse pubblico

I dati del fondo d’istituto con nomi e importi possono essere pubblicati.

Cedolini dello stipendio nel rispetto della privacy

(Comunicato stampa del GARANTE)

I "cedolini" dello stipendio dei lavoratori devono rispettare la privacy e, a questo fine, i datori di lavoro dovranno adottare le necessarie misure a tutela della riservatezza dei dati in essi contenuti.

(utilizzare delle buste chiuse)

Cartellini identificativi dei lavoratori a contatto con il pubblico

(Comunicato stampa del GARANTE)
Chiedere a lavoratori, specie se a contatto con il pubblico, di esporre un cartellino che li renda identificabili per finalità di trasparenza e di verifica del corretto funzionamento di aziende ed uffici pubblici, non contrasta con la legge sulla protezione dei dati personali.

E-mail

Tutte le E-mail inviate per conto della scuola devono contenere l'apposita dicitura contro lo *"SPAM":*

Le informazioni contenute in questa comunicazione e gli eventuali documenti allegati hanno carattere confidenziale e sono a uso esclusivo del destinatario. Nel caso questa comunicazione Vi sia pervenuta per errore, Vi informiamo che la sua diffusione e riproduzione è contraria alla legge e preghiamo di darci prontamente avviso e di cancellare quanto ricevuto. Grazie.

Non si può comunicare il numero di telefono di qualcuno detenuto dall'ente

- (dalla Relazione annuale del Garante) Inoltre, ad integrazione di quanto già sostenuto in precedenti decisioni dell'Autorità in materia di divulgazione degli estremi identificativi delle utenze telefoniche, si è precisato che è possibile comunicare il numero di telefono di un dipendente, ad altro dipendente che lo richieda, solo nei casi particolari di necessità ed urgenza

Gerarchia delle Fonti Giuridiche

- Infine, non va mai dimenticato che circolari e decreti ministeriali sono di rango inferiore rispetto al Codice, *che è una legge,* e che quindi in caso di conflitto quest'ultimo ha il sopravvento nella gerarchia delle fonti giuridiche.

Figure funzionali

- "Titolare" il Dirigente Scolastico
- "Responsabile del trattamento dei dati" D.S.G.A. e/o altro dipendente designato dal Titolare.
- "Custode delle parole chiave" D.S.G.A. o dipendente designato con nomina

Avvertenze importanti finali

- Si tratta di una normativa che sicuramente

  crea carichi di lavoro in più.

- E' evidente che applicarla nei minimi dettagli richiede un lavoro eccezionalmente oneroso e un atteggiamento mentale faticosamente meticoloso.
- Si ritiene che dovrebbe essere sufficiente un approccio di diligente buon senso improntato a buona fede, che garantisca il rispetto dello spirito delle norme in modo che sia adeguatamente protetto ogni dato personale la cui conoscenza da parte di estranei potrebbe recare un danno anche astrattamente concepibile all'Interessato e che i diritti dell'Interessato stesso siano pienamente rispettati.

Grazie per l’attenzione