PRIVACY E SCUOLA

(MATERIALE RACCOLTO/INTEGRATO/MODIFICATO A CURA DI MAURO MARTELLI)

* DLgs n. 196 del 30 giugno 2003 - Codice in materia di protezione dei dati personali

* DM n. 305 del 7 dicembre 2006 - Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della

*** Direttiva privacy del Dipartimento Funzione Pubblica 11 febbraio 2005**

PRESIDENZA DEL CONSIGLIO DEI MINISTRI – DIPARTIMENTO DELLA FUNZIONE PUBBLICA –

Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali, con particolare riguardo alla gestione delle risorse umane. (Direttiva n. 1/2005). (*GU n. 97 del 28-4-2005*)

* Linee guida per il trattamento dei dati personali dei lavoratori pubblici - Deliberazione del Garante n. 23 del 14 giugno 2007 –

Un provvedimento ad hoc per la gestione del rapporto di lavoro in ambito pubblico che è stato pubblicato nella G.U. 161 del 13 luglio 2007 supplemento ordinario n. 159.

Il codice della privacy e le scuole

Considerazioni sul decreto legislativo n. 196/2003 in relazione all'attività delle scuole

Indice

Principi generali

I principi di carattere generale definiti dagli articoli 1 e 2 del nuovo codice sono i seguenti:

- chiunque ha diritto alla protezione dei dati personali che lo riguardano;
- il trattamento dei dati personali si deve svolgere nel rispetto dei diritti e delle libertà fondamentali, nonche' della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Di fondamentale importanza, per agire con equilibrio in una materia così complessa, è il principio posto dall'articolo 3 del codice (principio di necessità nel trattamento dei dati). **Il principio di necessità** richiede che i sistemi informativi e i programmi informatici vengano configurati riducendo al minimo l'utilizzazione di dati personali

e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Ciò significa che il trattamento dei dati è consentito solo se vi è una specifica necessità, che non possa essere soddisfatta con altri mezzi e che il trattamento deve riguardare il minimo dei dati necessari per raggiungere gli obiettivi prefissati, in condizioni di appropriata sicurezza.

Non vi è dubbio che prendere coscienza, in prospettiva, di questo importante principio, significa ridurre al minimo gli oneri e le incombenze legate all'attuazione delle disposizioni in materia di Privacy.

Le parole chiave della privacy

Il nuovo codice della Privacy definisce all'articolo 4 i principali concetti di riferimento in materia. Di seguito viene proposta una selezione dei termini più significativi, nell'ottica dell'applicazione della normativa in esame all'ambito scolastico:

- **"trattamento"** è 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;
- **"dato personale"** è 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;
- **"dati identificativi"** sono i dati personali che permettono l'identificazione diretta dell'interessato;
- **"dati sensibili"** sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale. I dati personali idonei a rivelare lo stato di salute e la vita

sessuale costituscono una sottocategoria di dati sensibili oggetto di particolari tutele da parte della normativa in esame;

- **“dati giudiziari”** sono i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale. In sostanza si tratta di dati personali che rivelano l’esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato;
- **"titolare"**: con questo termine si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nel nostro caso il titolare è la scuola (articolo 28). Questa titolarità si esercita ovviamente attraverso il suo legale rappresentante, vale a dire il Dirigente della scuola;
- **"responsabile",** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali. Va individuato fra coloro che, in base al proprio profilo professionale, sono in grado di garantire, per esperienza e capacità, il pieno rispetto delle disposizioni in materia di trattamento, sicurezza compresa. Più in generale, si tratta di persona, società, ente, associazione, organismo a cui il titolare affida, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare (articolo 29).
- **“incaricati”,** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile. Gli incaricati si devono attenere alle istruzioni impartite e la loro designazione è fatta per iscritto e individua puntualmente l'ambito del trattamento consentito (articolo 30).

- **"interessato" è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali**, ed è dunque colui che esercita tutti i diritti relativi (quindi, se un trattamento riguarda, ad es., l'indirizzo, il telefono ecc. di Mario Rossi o della Spa XYZ, Mario Rossi e la Spa XYZ sono gli "interessati");
- **"comunicazione",** è il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **"diffusione"** è il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **"dato anonimo"** é il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- **"comunicazione elettronica"** è ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Diritti dell'interessato

Il Codice in materia di protezione dei dati personali riconosce all'interessato (articolo 7) una serie di diritti per quanto riguarda il trattamento dei dati personali:

a) **il diritto di accesso** ai propri dati personali direttamente presso chi li detiene (titolare del trattamento), ossia il diritto di ottenere la conferma della loro esistenza e la loro comunicazione e di sapere da dove sono stati acquisiti e quali sono i criteri e gli scopi del trattamento;

b) **il diritto di ottenere la cancellazione o il blocco** di dati che sono trattati violando la legge (ad es., perché non è stato chiesto il consenso); tali diritti possono essere esercitati anche quando non ci sono più motivi validi per conservare i dati;

c) **il diritto di aggiornare, correggere o integrare** i dati inesatti e incompleti;

d) il diritto, nei casi indicati nelle lettere b) e c), di ottenere anche un'attestazione da parte del titolare che tali operazioni sono state portate a conoscenza dei soggetti ai quali i dati erano stati precedentemente comunicati, a meno che ciò risulti impossibile o richieda un impegno sproporzionato rispetto al diritto tutelato;

e) il diritto di opporsi, per motivi legittimi, al trattamento dei propri dati;

f) **il diritto di opporsi al trattamento dei propri dati per scopi di informazione commerciale** o per l'invio di materiale pubblicitario o di vendita diretta, oppure per ricerche di mercato.

I diritti di cui sopra sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale e' fornito idoneo riscontro senza ritardo (articolo 8). L'esercizio dei diritti, quando non riguarda dati di carattere oggettivo, **può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo,** nonchè l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento (articolo 8, comma 4). I diritti dell'interessato devono essere richiamati nell'informativa di cui all'articolo 13 (si veda più avanti)

L'interessato può esercitare i suoi diritti con richiesta rivolta al titolare o al responsabile che può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica (articolo 9). Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2 (conferma esistenza dati, comunicazione all'interessato dei dati stessi, origine dei dati, finalità e modalità e logica del trattamento, estremi identificativi di titolare e responsabile, soggetti a cui i dati possono essere comunicati) **la richiesta può essere formulata anche oralmente** e in tal caso e' annotata sinteticamente a cura dell'incaricato o del responsabile.

Il codice dispone che per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento e' tenuto ad adottare idonee misure (articolo 10) volte, in particolare:

- ad agevolare l'accesso ai dati personali da parte dell'interessato
- a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente.

I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi e' richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica. Va tenuto presente che quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può

avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

Come devono essere trattati i dati

I dati personali oggetto di trattamento devono essere (articolo 11):

a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e **non eccedenti** rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati. E' importante notare che:

- **le disposizioni del Codice non si applicano ai trattamenti "per fini esclusivamente personali"** (ad eccezione della diffusione, si veda l'articolo 5, comma 3); quindi i trattamenti effettuati per gestire la propria agenda elettronica o cartacea, oppure una rubrica, o la propria posta personale non rientrano nell'ambito di applicazione delle norme sulla privacy. Vi sono poi altri trattamenti (ad es., quelli effettuati dal Centro elaborazione dati del Dipartimento di pubblica sicurezza, dagli uffici giudiziari per ragioni di giustizia, quelli effettuati per scopi di difesa o sicurezza dello Stato ovvero dalle forze di polizia per la prevenzione e il perseguimento di reati) che sono soggetti solo in parte all'applicazione delle disposizioni della legge sulla privacy;
- **le norme si applicano a tutti i trattamenti indipendentemente dal fatto che siano effettuati con l'ausilio di mezzi elettronici o comunque automatizzati**.

La protezione dei dati e le scuole

Il Codice in materia di protezione dei dati personali **interessa anche le istituzioni scolastiche** in quanto si applica al trattamento di dati personali, effettuato da **chiunque è stabilito nel territorio dello Stato** o in un luogo comunque soggetto alla sovranità dello Stato (articolo 5, comma 1). Quindi le regole fin qui citate si applicano anche alle istituzioni scolastiche. In aggiunta a queste, il codice prevede

regole ulteriori per i soggetti pubblici (articoli dal 18 al 22) che, ovviamente, **si applicano alle scuole di ogni ordine e grado in quanto esse sono amministrazioni pubbliche**, come definite dall'articolo 1, comma 2, del D.Lgs. n. 165/2001. Il D.Lgs n. 165/2001, lo ricordiamo, è il testo normativo fondamentale sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.

I principi generali applicabili a tutti i trattamenti effettuati da soggetti pubblici sono elencati nell'articolo 18; nei successivi articoli 19 (dati diversi da quelli sensibili e giudiziari), 20 (dati sensibili), 21 (dati giudiziari), 22 (altri principi applicabili ai dati sensibili e giudiziari), dettano ulteriori disposizioni le quali, integrate con quelle espressamente previste dal decreto nella Parte II, Titolo VI Istruzione, articoli 95 e 96, possono essere **compendiate**, in relazione all'attività delle scuole pubbliche, come segue:

- le scuole **non sono obbligate a notificare al Garante** il trattamento di dati personali, poiché i dati che trattano **non rientrano** tra le categorie per le quali è previsto l'obbligo di notifica (si veda l'articolo 37, comma 1, lettere da a) a f) o, se vi rientrano (come, ad esempio, i dati idonei a rivelare lo stato di salute, lettera b), i fini del trattamento sono diversi da quelli ivi indicati;
- **le scuole non devono richiedere il consenso** dell'interessato per effettuare il trattamento (articolo 18, comma 4);
- qualunque trattamento (di qualunque tipo di dati) è **consentito soltanto per lo svolgimento di funzioni istituzionali** (articolo 18, comma 2). Le funzioni che le scuole svolgono sono quelle che perseguono il fine istituzionale delle scuole stesse, cioè il fine "istruzione e formazione" degli alunni: quindi vi rientrano **tutte le funzioni individuate come pertinenti alle scuole dalla normativa vigente in materia di istruzione e formazione** (D.Lgs. n. 297/94, D.P.R. n. 275/1999, Legge n. 53/2003 e altre norme collegate) **e tutte quelle ad esse strumentali** (servizi generali e amministrativi), **incluse quelle che attengono al rapporto di lavoro con i dipendenti**;
- per quanto riguarda i **dati diversi da quelli sensibili e giudiziari** il relativo trattamento è consentito, per i fini istituzionali, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente (articolo 19, comma 1). **Attenzione**, vi sono **due eccezioni**:
  - la comunicazione da parte delle scuole **ad altri soggetti pubblici** è ammessa quando è prevista da una norma di legge o di regolamento (articolo 19, comma 2). In mancanza di una norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento delle funzioni istituzionali della scuola;

- la comunicazione **a soggetti privati** (od a enti pubblici economici) e la diffusione dei dati da parte delle scuole sono ammesse unicamente quando sono previste da una norma di legge o di regolamento (articolo 19, comma 3); ciò significa che sono praticamente vietate, ad eccezione di quanto espressamente previsto dall'articolo 96 circa la comunicazione e la diffusione, *"anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari"*. L'eccezione - che riguarda esclusivamente ***"le scuole e gli istituti scolastici di istruzione secondaria"*** - è consentita, però, **a due condizioni:**
    1. che la **finalità** del trattamento sia quella di *"agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero,"* degli alunni, e che tale finalità sia rispettata anche da chi riceve o raccoglie i dati in questione per il successivo trattamento da parte sua;
    2. che la comunicazione o la diffusione avvengano ***"su richiesta degli interessati"*** e che i dati oggetto di trattamento siano *"indicati nell'**informativa** resa agli interessati ai sensi dell'articolo 13"* (sull'informativa torneremo più avanti).

  Per quanto attiene specificamente alla **pubblicazione degli esiti scolastici**, l'articolo 96 (al comma 2), nel ribadire il *"diritto dello studente alla riservatezza"* (già stabilito dallo *"Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria"* adottato con D.P.R. n. 249/1998), mantiene ferme le *"vigenti disposizioni"*. Riteniamo pertanto **che sia legittima la pubblicazione degli esiti (anche se negativi) degli scrutini e degli esami, votazioni incluse (come avviene negli istituti di istruzione superiore),** e che essa non violi le norme sulla privacy. D'altro canto, rendere noti nominativamente gli esiti scolastici mediante affissione all'albo dell'istituto (che comporta la loro diffusione), risponde ad esigenze di trasparenza e di controllo sull'attività delle scuole che possono essere soddisfatte in pieno solo mediante la conoscenza delle valutazioni finali che le scuole stesse assegnano ai loro alunni. **Sulla pubblicazione degli esiti negativi** esiste peraltro il comportamento prudenziale delle scuole - adottato per disposizione dell'O.M. annuale sugli scrutini e gli esami (O.M. 21.5.2001, n. 90, art 16, confermata anche negli aa.ss. successivi al 2000/01) - di definire apposite modalità di **comunicazione preventiva alle famiglie dell'esito negativo di scrutini e di esami**, evitando poi - al momento della pubblicazione - l'indicazione esplicita dei voti e sostituendola con il **riferimento sintetico al risultato negativo** riportato dall'alunno (p.es. *non ammesso alla classe successiva,* etc.).

Attenzione però a due tipologie di dati personali la cui diffusione costituisce violazione della privacy, poiché rientrano nella categoria dei dati sensibili:

3. il dato circa la **volontà dell'alunno di avvalersi o meno dell'insegnamento della religione cattolica**; esso è *"idoneo a rivelare .... le convinzioni religiose"* (dato sensibile ai sensi dell'articolo 4, comma 1) e pertanto, a nostro avviso, non va pubblicato all'albo;
4. qualsiasi dato che permetta la identificazione, in sede di diffusione mediante pubblicazione all'albo, di **alunni portatori di handicap**. I **dati idonei a rivelare lo stato di salute**, che costituiscono una particolare sottocategoria di dati sensibili, sono tutelati in maniera speciale dalle norme del codice (qualche autore li definisce per questo "dati super sensibili"): essi infatti, a norma dell'articolo 22, comma 8, non possono essere diffusi. Il dato relativo al fatto che l'alunno portatore di handicap ha seguito un Piano Educativo Individualizzato va riportato, quindi, esclusivamente sulla documentazione interna alla scuola (registro dei voti) o sui certificati che vengono rilasciati all'interessato al termine del percorso di studi.

- per quanto attiene ai **dati sensibili e giudiziari**, il principio generale valido per i soggetti pubblici (e, quindi, per le scuole) è quello secondo il quale il trattamento *"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."* (articolo 20, comma 1 e articolo 21, comma 1). Per quanto attiene alle *"finalità di rilevante interesse pubblico"* la espressa disposizione di legge esiste ed è contenuta nello stesso codice (articolo 95): *"Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario, con particolare riferimento a quelle svolte anche in forma integrata."*.
  Si considerano, inoltre, di rilevante interesse pubblico, per quanto previsto dagli articoli 20 e 21, *"le finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo"*: si veda per questo l'articolo 112, che elenca anche i trattamenti per i quali è consentito ai soggetti pubblici trattare dati sensibili e giudiziari nell'ambito della gestione dei rapporti di lavoro;
- **i dati idonei a rivelare lo stato di salute** vanno conservati separatamente dagli altri dati personali (articolo 22, comma 7).

L'informativa all'interessato

Con il termine di *"informativa"* (si veda l'articolo 13) si intendono tutte le informazioni che il titolare del trattamento deve fornire ad ogni interessato verbalmente o per iscritto, quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi. In particolare:

- quali sono gli scopi e le modalità del trattamento;
- se l'interessato è obbligato o no a fornire i dati;
- quali sono le conseguenze se i dati non vengono forniti;
- a chi possono essere comunicati o diffusi i dati;
- quali sono i diritti riconosciuti all'interessato;
- chi sono il titolare e il responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax ecc.).

Nel fornire l' informativa i soggetti pubblici devono fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale e' effettuato il trattamento dei **dati sensibili e giudiziari** (articolo 22, comma 2).

L'informativa è obbligatoria e la sua omissione (o la sua inidoneità) è oggetto di pesante **sanzione amministrativa** (articolo 161). E' quindi necessario predisporla. E' opportuno, inoltre, che gli interessati, all'atto della acquisizione dei dati da parte della scuola, rilascino una dichiarazione che attesti di aver ricevuto e letto l'informativa fornita dalla scuola stessa.

L'informativa può essere differenziata in relazione alle diverse tipologie di interessati con cui la scuola intrattiene rapporti:

- con gli alunni e le loro famiglie (vedi modello in allegato n. 1);
- con il personale dipendente (vedi modello in allegato n. 2);
- con le aziende fornitrici di beni e servizi, gli enti e le associazioni (vedi modello in allegato n. 3). In questo caso non è prevista la rilevazione di dati sensibili.

I modelli presentati sopra sono puramente indicativi.

Un possibile modello organizzativo per il trattamento dei dati nelle scuole

Abbiamo già detto del titolare, che nelle amministrazioni pubbliche (e la scuola è fra esse) è individuato - dal codice - come la struttura *"nel suo complesso"* (articolo 28). **La titolarità è esercitata dal dirigente**, poiché è il legale rappresentante dell'istituzione ed a lui è demandata per legge (art. 4, comma 2, D.Lgs. n. 165/2001) *"la gestione finanziaria, tecnica e amministrativa"*, di cui è responsabile. Al dirigente competono inoltre *"le determinazioni per l'organizzazione degli uffici"* (art. 5, comma 2, D.Lgs. n. 165/2001). Va notato a questo proposito, che i criteri che devono ispirare l'organizzazione delle pubbliche amministrazioni *"sono attuati nel rispetto della disciplina in materia di trattamento dei dati personali"*, come stabilisce il codice introducendo un'apposita norma nel D.Lgs. n. 165/2001. Al dirigente competono quindi le decisioni in ordine al trattamento dei dati personali da parte della scuola e la vigilanza sull'applicazione delle norme in materia di protezione dei dati personali di cui la scuola è in possesso.
Ciò detto, non è pensabile che il dirigente effettui egli stesso il trattamento dei dati. Il codice individua, a questo proposito, altre figure:

- il responsabile, che è preposto dal titolare al trattamento dei dati e lo effettua attenendosi alle disposizioni impartite dal titolare (articolo 29);
- gli incaricati, che sono autorizzati (dal titolare o dal responsabile, che impartiscono loro le necessarie istruzioni) ad effettuare materialmente le operazioni di trattamento (articolo 30).

Possiamo ipotizzare - esclusivamente a titolo esemplificativo - un modello di organizzazione degli uffici che prevede, per esempio, quattro aree:

1. Area didattica, nella quale vengono trattati i dati relativi agli alunni, con gestione di dati sensibili (p.es. dati sull'handicap);
2. Area del personale, gestione del personale, con presenza di dati sensibili (p.es. dati sullo stato di salute o sull'adesione ai sindacati);
3. Area contabilità e finanza: gestione del bilancio, gestione fornitori: non dovrebbe comportare la presenza di dati sensibili;
4. Area degli affari generali: protocollo, archivio, rapporti con enti esterni (potrebbe trattare dati sensibili)

E' ovvio che **gli impiegati** (assistenti amministrativi) addetti alle singole aree **siano identificati quali incaricati** delle operazioni relative al trattamento dei dati e autorizzati in tal senso (per iscritto) con *"l'individuazione puntuale dell'ambito del*

trattamento consentito" (articolo 30, comma2). Possono ovviamente esserci altri incaricati (p.es. assistenti tecnici o persone esterne addetti ad operazioni sulle macchine elettroniche o sulla rete di computer etc., i quali possono venire a conoscenza dei dati nello svolgimento delle loro funzioni).
Nella scuole gli impiegati operano sotto la diretta responsabilità del Direttore dei Servizi Generali e Amministrativi (DSGA), al quale può esser quindi assegnato il ruolo di responsabile del trattamento, i cui compiti vanno anch'essi definiti per iscritto. Sempre a titolo di esempio, considerando che l responsabile del trattamento ha principalmente un ruolo di istruttoria, coordinamento e controllo, i suoi compiti potrebbero consistere in: sovrintendere all'attuazione delle istruzioni generali impartite dal titolare del trattamento per l'attuazione della legge, individuare gli incaricati del trattamento dei dati e fornire agli stessi istruzioni per la corretta esecuzione delle relative operazioni, riportare al dirigente le problematiche di maggior rilievo per una decisione in merito, collaborare con il titolare alla redazione ed all'aggiornamento del Documento Programmatico sulla Sicurezza (vedi più avanti), assicurarsi che le disposizioni emanate siano osservate, e così via.

Misure di sicurezza

Il codice dispone che i *"I dati personali* (a prescindere dal fatto che siano trattati in forma elettronica) *oggetto di trattamento sono custoditi e controllati,.... 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"* (articolo 31)

Il codice individua inoltre le cosiddette **"MISURE MINIME DI SICUREZZA"** (articoli 33, 34, 35 e 36) per il trattamento dei dati, **che i titolari devono adottare entro il 30 Giugno 2004.**

A tal fine l'articolo 34 del codice dispone che **il trattamento di dati personali effettuato con strumenti elettronici** e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a. autenticazione informatica;
b. adozione di procedure di gestione delle credenziali di autenticazione;
c. utilizzazione di un sistema di autorizzazione;

d. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f. adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g. tenuta di un documento programmatico sulla sicurezza (**DPS**); **il documento va predisposto entro il 30 giugno 2004 e poi aggiornato entro il 31 marzo di ogni anno successivo**

h. adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari **(non riguarda, pertanto, le scuole)**

A tal fine risulta fondamentale la lettura dell'allegato b) al codice, che contiene una serie di regole tecniche da rispettare, con particolare riguardo alla redazione del documento programmatico sulla sicurezza (regola 19). A tal fine il Garante ha predisposto un documento di guida alla redazione del DPS, in cui sono contenuti utili spunti e criteri per l'impostazione del DPS, per facilitare l'adempimento di questo obbligo da parte di organizzazioni non dotate al proprio interno di competenze specifiche.

Il documento predisposto dal Garante - che non è prescrittivo, ma secondo noi è molto utile per un approccio rapido e razionale al problema - descrive un percorso (basato sulla regola 19 dell'allegato B) che parte dall'autoanalisi delle tipologie di trattamento dei dati che si effettuano nell'attività dell'organizzazione, suggerendo il metodo di individuare e inserire in tabelle, di cui fornisce un esempio, tutti gli elementi atti ad individuare sinteticamente i trattamenti effettuati e gli strumenti utilizzati; con la stessa metodologia sono quindi descritti:

- la distribuzione dei compiti e delle responsabilità
- l'analisi dei rischi che incombono sui dati
- le misure di sicurezza in essere e quelle da adottare
- i criteri e le modalità di ripristino dei dati in caso di danneggiamento
- la pianificazione degli interventi formativi previsti
- i trattamenti eventualmente affidati all'esterno.

Nell'ipotesi, infine, in cui il trattamento sia eseguito senza l'ausilio di strumenti elettronici esso e' consentito solo se sono adottate, sempre nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Responsabilità civile e sanzioni amministrative

La responsabilità civile per danni cagionati per effetto del trattamento è regolata dall'articolo 15 del codice, che equipara il trattamento dei dati all'esercizio di attività pericolose, prevedendo il risarcimento ai sensi dell'articolo 2050 del Codice Civile, che riportiamo di seguito:

Codice Civile, art. 2050 **Responsabilità per l'esercizio di attività pericolose.**
"*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 avere adottato tutte le misure idonee a evitare il danno.***"

Di qui il ruolo rilevante dell'adozione di idonee misure di sicurezza come quelle previste dal disciplinare tecnico contenuto nell'allegato B.

L'articolo 161 dispone che la violazione delle disposizioni di cui all'articolo 13 del codice (obbligo e contenuto dell' informativa) 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, 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.

L'articolo 162 dispone che la cessione illegittima dei dati è punita con la sanzione amministrativa del pagamento di una somma da cinque mila a trentamila euro.

In questi casi può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o piu' giornali indicati nel provvedimento che la applica.

L'organo competente ad irrogare le sanzioni è il Garante.

Illeciti penali

L'articolo 167 comma 1 del codice dispone che, salvo che il fatto costituisca piu' grave reato, chiunque, **al fine di trarne per se' 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, (principi generali relativi ai soggetti pubblici, trattamento dati non sensibili da parte di soggetti pubblici, comunicazioni elettroniche) e' 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 sei a ventiquattro mesi.

L'articolo 167 comma 2 dispone che salvo che il fatto costituisca piu' grave reato, chiunque, **al fine di trarne per se' 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 (trattamento dati sensibili da parte di soggetti pubblici, trattamento dati giudiziari, diffusione dati sullo stato di salute, test attitudinali), e' punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

I reati di cui sopra si concretizzano se c'è la volontarietà del soggetto che ha agito (dolo specifico).

L'articolo 169 dispone che chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 (misure minime di sicurezza) e' punito con l'arresto sino a due anni o con l'ammenda da diecimila a cinquantamila euro.

Direttiva privacy del Dipartimento Funzione Pubblica

PRESIDENZA DEL CONSIGLIO DEI MINISTRI – DIPARTIMENTO DELLA FUNZIONE PUBBLICA – DIRETTIVA 11 febbraio 2005

Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali, con particolare riguardo alla gestione delle risorse umane. (Direttiva n. 1/2005). (*GU n. 97 del 28-4-2005*)

Alla Presidenza del Consiglio dei Ministri - Segretariato generale
Alle Amministrazioni dello Stato anche ad ordinamento autonomo
Al Consiglio di Stato - Ufficio del Segretario generale
Alla Corte dei conti - Ufficio del Segretario generale
All'Avvocatura generale dello Stato - Ufficio del Segretario generale
Alle Agenzie di cui al decreto legislativo n. 300/1999
All'ARAN
Alla Scuola superiore della pubblica amministrazione
Agli enti pubblici non economici (tramite i Ministeri vigilanti)
Agli enti di pubblici (ex art. 70 del d.lgs. n. 165/2001)
Agli enti di ricerca (tramite il Ministero dell'istruzione, dell'università e della ricerca)
Alle istituzioni universitarie (tramite il Ministero dell'istruzione, dell'università e della ricerca)
e, per conoscenza
All'ANCI
All'UPI
All'UNCEM
Alla Conferenza dei presidenti
delle regioni
Alla Conferenza dei rettori delle università italiane

1. Premessa.

Il primo gennaio del 2004 é entrato in vigore il decreto legislativo 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali», d'ora in poi denominato «Codice», nel quale sono raccolte, in forma di testo unico, tutte le disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ed alle attività connesse.

Il Testo rappresenta il primo modello di codificazione organica della privacy in Europa e tiene conto sia del quadro normativo comunitario (direttive n. 95/46/CE e n. 2002/58/CE) che di quello internazionale.

La disciplina del Codice, analogamente a quella dettata dalla normativa previgente, si innesta in un contesto prevalentemente orientato alla pubblicità dell'azione amministrativa, ad opera della legge 7 agosto 1990, n. 241, e delle altre disposizioni di settore, e conferma la graduazione dei differenti livelli di tutela previsti all'interno della generale categoria dei dati personali predisponendo garanzie più rigorose in relazione ai dati sensibili.

Il Codice offre al cittadino un sistema di garanzie articolato e al contempo semplificato che, nell'individuare tutti gli strumenti idonei ad una piena realizzazione del diritto alla protezione dei dati personali, costituisce il presupposto per la fruizione di tutti gli altri diritti fondamentali dell'individuo che a quel diritto sono naturalmente collegati.

In tale quadro i principi ricordati nel testo unico informano tutti gli aspetti della vita sociale e dell'azione delle pubbliche amministrazioni ed in particolare, per quanto interessa in questa sede, anche gli aspetti relativi alla gestione delle risorse umane in tutti gli aspetti organizzativi, di sicurezza e di benessere.

2. I Principi e gli obblighi.

Appare opportuno ricordare in questa sede i principi che derivano dal Codice in materia di protezione dei dati personali ai quali l'azione

amministrativa dovrà ispirarsi e che sono destinati ad esercitare una grande influenza sull'esercizio della potestà organizzativa delle pubbliche amministrazioni.

Il «diritto alla protezione dei dati personali» quale prerogativa fondamentale della persona, é stato introdotto nell'ordinamento in attuazione dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000 e deve considerarsi quale diritto autonomo e distinto rispetto al diritto alla riservatezza sostanziandosi nel diritto del suo titolare di conoscere e controllare la circolazione delle informazioni che lo riguardano.

Il Codice, che ha dunque affermato, all'art. 1, il diritto alla protezione dei dati personali, mira a garantire che il trattamento di queste informazioni «si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali» (art. 2).

Un principio generale del sistema di garanzie approntato dal Codice che deve guidare l'azione amministrativa é costituito dal principio di «necessità del trattamento dei dati personali», da intendersi quale principio che integra quello di «pertinenza e non eccedenza» dei dati trattati (già individuato dalla legge n. 675 del 1996) con riferimento alla configurazione di sistemi informativi e programmi informatici. Tale regola prescrive di predisporre i sistemi informativi e i programmi informatici in modo da utilizzare al minimo dati personali ed identificativi escludendone il trattamento quando le finalità perseguite possono essere raggiunte mediante l'uso di dati anonimi o di modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3). Deve essere, inoltre, ricordato che il principio di necessità costituisce un presupposto di liceità del trattamento dei dati personali ed il mancato rispetto di questo e degli altri presupposti comporta conseguenze rilevanti per l'amministrazione. Infatti il Codice, nel dettare le regole per tutti i trattamenti ha sancito l'inutilizzabilità dei dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali (art. 11, comma 2).

Il diritto alla protezione dei dati personali potrà, pertanto, essere garantito solo se le amministrazioni titolari dei trattamenti ispireranno la loro attività ai principi sanciti dal Codice e conseguentemente, oltre ad ottemperare agli obblighi espressamente previsti, adotteranno una serie di comportamenti concreti, azioni e provvedimenti organizzativi coerenti con i principi che regolano la materia.

In particolare, il trattamento dei dati personali da parte delle pubbliche amministrazioni é consentito solo qualora sia necessario per lo svolgimento delle funzioni istituzionali rispettando gli eventuali altri presupposti e limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti. Al riguardo é il caso di sottolineare che, salvo quanto previsto per i trattamenti posti in essere dagli esercenti le professioni sanitarie e gli organismi sanitari pubblici (parte II del Codice), le pubbliche amministrazioni non devono chiedere il consenso dell'interessato.

I dati sensibili possono, invece, essere trattati soltanto se il trattamento risulta autorizzato da un'espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite (articoli 18, 19, 20 e 22 del Codice.

Per i dati sensibili v. più diffusamente infra la parte relativa ai «Regolamenti»).

É inoltre, imposto alle amministrazioni l'obbligo di garantire la sicurezza nella gestione dei dati e dei sistemi in modo da ridurre al minimo 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. Pertanto le amministrazioni, o i soggetti affidatari di servizi e sistemi per conto delle stesse, dovranno adottare tutte le cautele consentite dalle moderne tecnologie prevenendo i rischi derivanti dall'organizzazione e gestione delle banche dati e dei sistemi informativi (articoli 3135 e disciplinare tecnico contenuto nell'allegato B al Codice). Analoghe cautele dovranno essere adottate nella gestione di tutti gli atti ed i provvedimenti che comportano l'utilizzo di dati personali e sensibili.

Nell'ambito del predetto obbligo generale di contenere nella misura più ampia possibile determinati rischi, i titolari del trattamento sono tenuti in ogni caso ad assicurare un livello minimo di protezione dei dati mediante

l'adozione delle «misure minime» di sicurezza individuate nel Titolo V, Capi I e II, della Parte II del Codice o che saranno individuate ai sensi dell'art. 58, comma 3, in relazione ai trattamenti effettuati per finalità di difesa o coperti da segreto di Stato.

La disciplina del Codice, infine, é informata dal principio di semplificazione in base al quale l'elevato grado di tutela dei diritti é assicurato nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità di esercizio del diritto alla protezione dei dati personali e degli altri diritti e libertà fondamentali dell'interessato e degli adempimenti in capo ai titolari del trattamento (art. 2, comma 2).

Disposizioni in deroga o ad integrazione della disciplina generale sono poste dal Codice in relazione a specifici settori di interesse per l'attività amministrativa, quali l'ambito giudiziario, negli articoli da 46 a 52, i trattamenti eseguiti dalle forze di polizia, negli articoli da 53 a 57, e quelli attinenti alla difesa e sicurezza dello Stato, di cui all'art. 58.

3. Finalità della direttiva.

La presente direttiva é finalizzata a richiamare l'attenzione delle amministrazioni sulle prescrizioni del Codice che incidono maggiormente nel settore pubblico, richiedendo **l'adozione di efficaci scelte organizzative** per tradurre sul piano sostanziale le garanzie previste dal legislatore, nonché sulle conseguenze connesse alla loro mancata attuazione.

L'entrata in vigore del nuovo Codice comporta, per le pubbliche amministrazioni, la necessità di **ripensare le proprie attività e la propria organizzazione** al fine di consentire una piena ed effettiva garanzia dei diritti in esso affermati.

Infatti, le tematiche relative alla privacy investono le amministrazioni nella quasi totalità delle proprie attività, assumendo significativo rilievo nello svolgimento di molti dei compiti istituzionali loro affidati dall'ordinamento, come ad esempio, la gestione delle risorse umane.

In considerazione di ciò, il Codice (art. 176) ha aggiunto il comma 1-bis al comma 1 dell'art. 2 del decreto legislativo 30 marzo 2001, n. 165. Pertanto le amministrazioni **dovranno attuare le linee fondamentali di**

organizzazione degli uffici nel rispetto della disciplina in materia di trattamento dei dati personali, in aggiunta ai criteri indicati nella medesima disposizione.

Da quanto premesso emerge la necessità di provvedere all'adozione egli strumenti necessari per l'attuazione pratica delle previsioni del Codice, quali:

- **regolamenti indicanti i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che possono essere eseguite su di essi in relazione al perseguimento di finalità di rilevante interesse pubblico qualora manchi una specifica indicazione legislativa (articoli 20, 21 e 22);**
- **le informative all'interessato (art. 13);**
- **la notificazione al Garante nei casi previsti dall'art. 37;**
- **le eventuali comunicazioni al Garante (art. 39);**
- **le misure minime di sicurezza e, in particolare, il documento programmatico sulla sicurezza (art. 34, comma 1, lettera g) e regola n. 19 dell'allegato B al Codice).**

Occorrerà, inoltre, procedere a puntuali ricognizioni dei dati trattati alla luce delle disposizioni vigenti e **alla revisione delle modalità di gestione degli stessi**, ponendo particolare attenzione alla necessità di garantire agli interessati l'esercizio del diritto di accesso ai dati che li riguardano e degli altri diritti sanciti dall'art. 7 del Codice, nonché alle problematiche relative all'accesso ai documenti amministrativi ed alla necessità di contemperare le esigenze di trasparenza dell'azione amministrativa con quelle di tutela del diritto alla protezione dei dati personali.

Pertanto ci si rivolge ai dirigenti ed ai funzionari preposti alle unità di loro competenza perché nell'ambito delle attività di direzione, coordinamento e controllo degli uffici dei quali sono responsabili adottino tutte le misure utili a garantire il rispetto e la piena attuazione dei principi sanciti dal Codice, prevengano i rischi presenti nelle singole attività e adottino, conseguentemente, tutti gli atti, le soluzioni organizzative ed i comportamenti necessari.

4. Classificazione dei dati e tipologia dei relativi adempimenti.

4.1. Dati personali.

L'art. 4, comma 1, lettera b) del Codice definisce dati personali «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».

Alle pubbliche amministrazioni é consentito il trattamento dei dati personali quando risponda alla necessità di esercitare le proprie funzioni istituzionali. Pertanto, salvo quanto previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici (si vedano le disposizioni della parte II del Codice), le medesime **non debbono chiedere il consenso** dell'interessato ai sensi dell'art. 18.

In particolare, il trattamento dei dati diversi da quelli sensibili e giudiziari é consentito anche in assenza di una specifica previsione normativa purché sia finalizzato allo svolgimento delle funzioni istituzionali dell'amministrazione, mentre la comunicazione di questi dati da una pubblica amministrazione ad un'altra o a privati oppure la loro diffusione **é possibile solo quando vi sia una espressa previsione normativa, come indicato all'art. 19.**

Nel caso in cui le amministrazioni abbiano necessità di fornire tali informazioni ad un'altra pubblica amministrazione, sempre ai fini dello svolgimento delle attività istituzionali, ma in assenza di idonea previsione normativa, **possono però informarne preventivamente il Garante, ai sensi dell'art. 39 del Codice**. In base a tale nuovo meccanismo, decorsi quarantacinque giorni dalla comunicazione al Garante, l'operazione di comunicazione dei dati può essere avviata, ferma restando la possibilità di una diversa determinazione dell'Autorità adottata anche successivamente al decorso del termine.

Deve essere effettuata una preventiva comunicazione al Garante, a norma dell'art. 39, anche nel caso di trattamento di dati idonei a rivelare

lo stato di salute previsto da un programma di ricerca biomedica o sanitaria, conformemente a quanto dispone l'art. 110 del Codice.

Sulle amministrazioni titolari del trattamento grava inoltre l'obbligo di notificare al Garante i trattamenti di dati personali che sono elencati nel comma 1 dell'art. 37 del Codice. Tale adempimento deve essere effettuato prima dell'inizio del trattamento ed una sola volta, a prescindere delle operazioni che debbono essere effettuate (salvo, ovviamente, l'obbligo di notificare le eventuali modifiche del trattamento o la sua cessazione). In base agli articoli 37 e 38, la notificazione si intende validamente effettuata solo se inviata telematicamente utilizzando le modalità indicate dal Garante tramite il modello all'uopo predisposto e disponibile sul sito dell'Autorità (www.garanteprivacy.it). Al riguardo si segnala che, con provvedimento n. 1 del 31 marzo 2004, disponibile anch'esso sul sito dell'Autorità, sono stati individuati alcuni trattamenti di dati non suscettibili, in concreto, di recare pregiudizio agli interessati e quindi sottratti all'obbligo di notificazione di cui al citato art. 37.

Si rammenta infine che sulla base della disciplina del Codice configura una «comunicazione» di dati personali il dare conoscenza di tali informazioni ad uno o più soggetti diversi dall'interessato, in qualunque forma, **anche mediante la loro messa a disposizione o consultazione**. Non può considerarsi tale, invece, la comunicazione effettuata nei confronti dell'interessato, del rappresentante del titolare nel territorio dello Stato, del responsabile o dell'incaricato (art. 4, comma 1, lettera l).

4.2. Regole generali per il trattamento dei dati.

Le regole generali, comuni a tutti i trattamenti di dati, sono rinvenibili negli articoli da 11 a 17 del Codice.

4.2.1. Modalità del trattamento e requisiti dei dati.

In particolare, l'art. 11, nell'indicare le modalità del trattamento e i requisiti dei dati, individua anche i presupposti di liceità del trattamento. Secondo la disciplina introdotta dal Codice, il mancato rispetto dei

presupposti sanciti da tale disposizione e delle altre norme rilevanti in materia trattamento di dati personali **comporta l'inutilizzabilità dei dati** (art. 11, comma 2).

4.2.2. Titolare, responsabile, incaricati.

Per quanto riguarda i soggetti che effettuano il trattamento, l'art. 28 chiarisce che il «titolare del trattamento», nel caso delle pubbliche amministrazioni, coincide con l'entità nel suo complesso ovvero con l'unità o l'organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza, anziché con la persona fisica incardinata nell'organo o preposta all'ufficio.

Per le strutture amministrative complesse si suggerisce di avvalersi della facoltà accordata al titolare dall'art. 29 del Codice di designare uno o più «responsabili del trattamento», fra i soggetti che, per qualità professionali e personali, forniscano idonea garanzia del rispetto delle disposizioni vigenti in materia.

Tale designazione deve essere accompagnata dalla specificazione analitica per iscritto dei compiti affidati e dalla vigilanza periodica sulla puntuale osservanza delle istruzioni impartite e sul generale rispetto delle norme in materia di protezione dei dati personali, come previsto dal comma 5 dell'art. 29.

A chiusura del sistema é posta la previsione relativa agli «incaricati del trattamento», i soli che possono materialmente effettuare le operazioni di trattamento di dati personali. Gli incaricati operano sotto la diretta autorità del titolare o del responsabile, previa designazione espressa per iscritto, contenente la puntuale individuazione dell'ambito del trattamento loro consentito e l'indicazione delle istruzioni cui devono attenersi nello svolgimento del trattamento. **Per semplificare tale adempimento, in considerazione della frequenza con cui il personale viene soggetto a rotazione e avvicendamento all'interno delle strutture amministrative, il Codice considera equivalente alla designazione nominativa degli incaricati, la preposizione del personale ad un'unità organizzativa (ad esempio, tramite un ordine di servizio)**

per la quale venga altresì individuato per iscritto l'ambito del trattamento consentito agli addetti che operano all'interno della medesima unità.

4.2.3. Informativa agli interessati.

A tutela dell'esercizio del diritto alla protezione dei dati personali il Codice pone in capo ai titolari del trattamento l'obbligo, previsto dall'art. 13, di fornire agli interessati un'adeguata informativa. L'interessato o la persona presso la quale sono raccolti i dati personali deve pertanto essere informato oralmente o per iscritto, fra l'altro, delle finalità e delle modalità del trattamento dei dati, della eventuale obbligatorietà del loro conferimento, delle conseguenze relative al rifiuto di fornire i dati, dei diritti esercitabili dal medesimo interessato, nonché dei dati identificativi del titolare del trattamento e del responsabile. Nel caso di designazione di più responsabili, il Codice introduce un'ulteriore semplificazione dando possibilità di riportare nell'informativa all'interessato gli estremi identificativi di un solo responsabile indicando contestualmente le modalità attraverso le quali é conoscibile l'elenco completo e aggiornato dei responsabili (ad esempio, attraverso l'indicazione del sito istituzionale dell'amministrazione in cui l'elenco é eventualmente pubblicato).

4.3. Dati sensibili.

L'art. 4, comma 1, lettera d) del Codice definisce dati sensibili«i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale».

Il trattamento dei dati sensibili é consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati

che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite. Qualora una disposizione di legge non specifichi i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che possono essere svolte su di essi, le amministrazioni sono tenute ad identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili, in relazione al perseguimento di finalità ritenute dalla legge di rilevante interesse pubblico, aggiornando ed integrando tale identificazione periodicamente (art. 20, commi 1, 2 e 4, del Codice). Al riguardo, la parte II del Codice individua alcune attività di rilevante interesse pubblico, tra le quali assumono rilievo per le pubbliche amministrazioni, a titolo esemplificativo, le attività finalizzate all'applicazione della disciplina sull'accesso ai documenti amministrativi (art. 59), o della normativa in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti o abilitazioni (art. 68), le attività socio-assistenziali (art. 73) e quelle volte all'instaurazione e alla gestione da parte di soggetti pubblici di rapporti di lavoro (art. 112).

Nel caso in cui invece le amministrazioni intendano porre in essere un trattamento di dati sensibili che non risulti previsto espressamente da una disposizione normativa di rango primario, esse possono richiedere al Garante se siano ravvisabili i presupposti di rilevante interesse pubblico che ne autorizzano il trattamento, secondo il meccanismo previsto dall'art. 26, comma 2, del Codice. In tal caso, il trattamento é consentito soltanto se l'amministrazione interessata provveda altresì ad identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili con un atto di natura regolamentare (art. 20, comma 3, del Codice, al riguardo, v. più diffusamente infra la parte relativa ai «Regolamenti»).

4.4. Dati giudiziari.

L'art. 4, comma 1, lettera e) del Codice definisce «dati giudiziari» i dati personali idonei a rivelare provvedimenti iscrivibili nel casellario giudiziale indicati dall'art. 3, comma 1, lettere da a) ad o) e da r) ad u) del decreto del Presidente della Repubblica 14 novembre 2002, n. 313, o la qualità di

imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

É possibile per le pubbliche amministrazioni trattare tali informazioni quando ciò sia previsto da una norma di legge oppure da un provvedimento del Garante che specifichi espressamente le rilevanti finalità di interesse pubblico perseguite, i dati personali che possono essere utilizzati e le operazioni di trattamento eseguibili. Nel caso in cui la legge specifichi soltanto le finalità di rilevante interesse pubblico, valgono le prescrizioni relative al trattamento dei dati sensibili, di cui all'art. 20, commi 2 e 4, del Codice **per quanto riguarda la necessità di individuare e rendere pubblici attraverso un atto di natura regolamentare i tipi di dati utilizzabili e le operazioni eseguibili (art. 21).**

4.5. Regolamenti.

Gli articoli 20, comma 2, e 21, comma 2, del Codice prevedono che, quando una disposizione di legge abbia specificato le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che possono essere svolte su di essi, **le amministrazioni dovranno adottare un apposito regolamento con il quale identificare e rendere pubblici, a cura dei soggetti che ne effettuano il trattamento, i tipi di dati utilizzabili e le operazioni eseguibili, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dall'art. 22 del Codice**. L'adozione di tali provvedimenti postula la previa ricognizione di tutte le attività poste in essere dal soggetto pubblico che comportano un trattamento di dati sensibili o giudiziari, nonché la valutazione **della indispensabilità** dei dati utilizzati e delle operazioni svolte nell'ambito di tali attività rispetto alle finalità di volta in volta perseguite. I dati trattati vanno indicati per categorie (ad esempio, dati sulla salute, vita sessuale, sull'origine razziale, sull'origine etnica, ecc.**), tenendo conto che le tipologie di dati non individuate nel regolamento non potranno essere trattate.**

In altri termini, tramite tali regolamenti dovrà risultare chiaro ai cittadini il collegamento tra le finalità di rilevante interesse pubblico

perseguite dalle amministrazioni in relazione ai compiti ad esse attribuiti dall'ordinamento e le modalità con cui vengono effettivamente utilizzate le informazioni che li riguardano. Al fine di dare efficacia al sistema di garanzie delineato dal Codice per i dati sensibili e giudiziari é pertanto necessario che le amministrazioni provvedano a tale identificazione, ove mancante, tramite atti di natura regolamentare, entro il 31 dicembre 2005, previa acquisizione del parere di conformità del Garante ai sensi dell'art. 154, comma 1, lettera g), del Codice (art. 3, decreto-legge 24 giugno 2004, n. 158, convertito con legge 27 luglio 2004, n. 188, che modifica l'art. 181, comma 1, lettera a) del Codice).
L'identificazione dei tipi di dati e di operazioni é poi aggiornata e integrata periodicamente, come indicato dall'art. 20 del Codice.
Per rendere più agevole e rapida l'adozione di tali atti, **il Codice prevede che il parere del Garante possa essere formulato anche su schemi tipo. Nel caso in cui gli schemi regolamentari predisposti dalle amministrazioni corrispondano ai modelli su cui il Garante ha reso un parere conforme, non sarà quindi necessario sottoporli caso per caso allo specifico esame da parte dell'Autorità.**
A tal fine, si esortano le amministrazioni ad avviare ogni iniziativa utile ad identificare settori di attività, comuni a più amministrazioni, per i quali si possa procedere ad un'elaborazione congiunta di schemi tipo da sottoporre all'attenzione del Garante, anche attraverso i progetti che questo Dipartimento avvierà in collaborazione con il Formez.

4.6. Criteri applicabili al trattamento dei dati sensibili e giudiziari.

L'art. 22 indica i criteri applicabili al trattamento dei dati sensibili e giudiziari. In primo luogo, le pubbliche amministrazioni devono prestare particolare attenzione alla prevenzione di possibili danni per l'interessato, conformando il trattamento di queste informazioni in modo da prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

In tale contesto assume uno specifico rilievo **il principio di indispensabilità**, in base al quale possono essere trattati soltanto i dati sensibili e giudiziari indispensabili allo svolgimento di funzioni istituzionali che non potrebbero essere adempiute altrimenti (mediante il ricorso a dati anonimi o dati personali di diversa natura).

Analogamente, sui dati sensibili e giudiziari indispensabili, le amministrazioni possono effettuare unicamente le operazioni di trattamento strettamente necessarie al raggiungimento delle finalità consentite nei singoli casi.

Rispetto alla normativa previgente, é confermato infine il divieto di diffondere i dati idonei a rivelare lo stato di salute.

4.7. Sicurezza dei dati.

Una particolare attenzione é posta dal Codice, negli articoli 31 e seguenti, alle tematiche della sicurezza dei dati e dei sistemi.

Il Codice distingue in proposito le misure di sicurezza da adottare in:

- misure idonee e preventive volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31);
- misure minime, indicate negli articoli 34 e 35 secondo le modalità applicative analiticamente specificate nell'allegato B) al Codice e diversificate a seconda che il trattamento sia effettuato o meno con strumenti elettronici, ovvero da individuare, ai sensi dell'art. 58, comma 3, in relazione ai trattamenti effettuati per finalità di difesa o coperti da segreto di Stato (art. 33).

La distinzione rileva ai fini sanzionatori perché, mentre l'inosservanza delle misure «minime» configura una condotta penalmente rilevante, ai sensi dell'art. 169 del Codice, l'inosservanza delle misure «idonee» rende il trattamento illecito e, nel caso in cui si cagioni un danno all'interessato, espone l'autore del danno ad eventuali azioni risarcitorie da parte del soggetto leso (art. 15 del Codice).

In particolare, l'omessa adozione delle misure minime di sicurezza é punita con l'arresto sino a due anni o con l'ammenda da 10 mila euro a 50 mila euro. In questo caso é però previsto il meccanismo del «ravvedimento operoso» applicabile a coloro i quali adempiano puntualmente alle prescrizioni impartite dal Garante una volta accertato il reato ed effettuino un pagamento in sede amministrativa di una somma pari al quarto del massimo dell'ammenda, ottenendo così l'estinzione del reato.

4.8. Documento programmatico sulla sicurezza.

Fra le misure minime di sicurezza previste dal Codice rientra anche il Documento programmatico sulla sicurezza (Dps), **obbligatorio per chi effettua un trattamento di dati sensibili e giudiziari con l'ausilio di strumenti elettronici.** Tale documento deve contenere, in particolare, l'analisi dei rischi che incombono sui dati personali, l'individuazione degli accorgimenti da adottare per prevenire la loro eventuale distruzione, perdita accidentale o gli accessi abusivi e la pianificazione degli interventi formativi nei riguardi del personale.
Il Dps deve essere adottato, dall'organo, ufficio o persona fisica a ciò legittimata in base all'ordinamento dell'amministrazione e predisposto (o aggiornato per le amministrazioni che erano già tenute a redigere o ad aggiornare il Dps in base alla previgente disciplina) al più tardi entro il 30 giugno 2005 [rinviato al 31.12.2005 successivamente alla presente Direttiva- NDR] (art. 6, decreto-legge 9 novembre 2004, n. 266 che modifica l'art. 180 del Codice). Decorso il periodo transitorio connesso all'entrata in vigore del Codice, secondo quanto precisato dal Garante nel pareredel 22 marzo 2004, e, quindi a partire dal 2006, il termine per aggiornare annualmente il Dps rimarrà fissato alla scadenza del 31 marzo di ogni anno, come dispone la regola tecnica n. 19 dell'allegato B) al Codice.
Le amministrazioni che per obiettive ragioni di natura tecnica non possono, in tutto o in parte, applicare entro il 30 giugno 2005[rinviato al 31.03.2006 successivamente alla presente Direttiva - NDR] le misure minime introdotte dalla nuova disciplina con riferimento agli elaboratori elettronici e ai programmi utilizzati possono avvalersi di un termine più

ampio per l'adeguamento (30 settembre 2005, secondo quanto dispone l'art. 6 del decreto-legge citato), purché predispongano un documento, avente data certa, nel quale sono descritti tali impedimenti tecnici e lo conservino presso la propria struttura. Nell'attesa di adeguare la propria dotazione tecnologica, l'amministrazione é però tenuta ad adottare ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti, in modo da evitare i rischi, indicati dall'art. 31 del Codice, di distruzione, perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

5. Accesso ai dati e accesso ai documenti.

5.1. Accesso ai dati personali.

É opportuno rammentare alcuni elementi di rilievo introdotti dal Codice in materia di accesso ai dati personali. Com'é noto, il Codice riconosce all'interessato vari diritti nei confronti delle pubbliche amministrazioni che trattano i suoi dati personali, tra cui, in particolare, il diritto di accedere ai dati che lo riguardano, di ottenerne l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in forma anonima o il blocco se trattati in violazione di legge, di opporsi al trattamento per motivi legittimi (art. 7).

Per esercitare tali diritti l'interessato deve presentare una richiesta all'amministrazione titolare del trattamento (o al responsabile, qualora l'amministrazione si sia avvalsa di tale facolta) senza particolari formalità (art. 9). La richiesta, se non fa riferimento ad un particolare trattamento o a specifici dati o categorie di dati personali, deve ritenersi riferita a tutti i dati personali che riguardano l'interessato comunque trattati dall'amministrazione (art. 10) e può riguardare anche informazioni di tipo valutativo, salvo per quanto attiene alla loro rettifica o integrazione (art. 8, comma 4).

L'amministrazione destinataria della richiesta é tenuta a fornire un riscontro compiuto ed analitico all'interessato nel termine di 15 giorni dal suo ricevimento, ovvero di 30 giorni, dandone comunicazione all'interessato, se le operazioni necessarie per un integrale riscontro sono

di particolare complessità o se ricorre altro giustificato motivo (art. 146). Il riscontro può essere fornito anche oralmente, tuttavia, in presenza di una specifica istanza, l'amministrazione é tenuta a trasporre i dati su supporto cartaceo o informatico o a trasmetterli all'interessato per via telematica (art. 10).

Si esortano pertanto le amministrazioni a predisporre idonei meccanismi e procedure volti a dare piena attuazione alle disposizioni del Codice in materia di accesso ai dati, in modo da agevolare l'accesso da parte degli interessati alle informazioni che li riguardano, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad una accurata selezione dei dati relativi a singoli soggetti, e da semplificare le modalità e ridurre i tempi per il riscontro agli interessati anche nell'ambito degli uffici per le relazioni con il pubblico.

5.2. Accesso ai dati e accesso ai documenti amministrativi.

Occorre sottolineare, infine, alcuni elementi che differenziano il diritto di accesso ai dati personali e gli altri diritti introdotti dalla disciplina sulla protezione dei dati personali dal diritto di accesso ai documenti amministrativi previsto dagli articoli 22 e seguenti della legge n. 241/1990 e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione. Si tratta, infatti, come ricordato più volte dal Garante, di due diversi ed autonomi diritti di accesso che differiscono in termini di oggetto e di presupposti del loro esercizio.

Il diritto di accesso ai dati personali e gli altri diritti sanciti dal Codice riguardano i dati personali (anziché ad atti e documenti) e possono essere esercitati dalle persone cui i dati si riferiscono senza particolari formalità e limitazioni, ad eccezione di taluni diritti che richiedono una specifica situazione (ad esempio, la rettifica può essere richiesta solo in relazione a dati inesatti e la cancellazione solo nei confronti di dati utilizzati in violazione di legge) e dei casi di esclusione tassativamente indicati dal Codice (art. 8). In particolare, ai fini dell'esercizio del diritto di accesso ai dati, l'interessato non é tenuto ad esplicitare le ragioni della sua richiesta di accesso, che può concernere soltanto le informazioni

riferite alla propria persona e non può essere estesa ai dati relativi a terzi.

Il diritto di accesso ai documenti é, invece, garantito solo in riferimento a documenti della pubblica amministrazione e di determinati altri soggetti da parte di chiunque sia portatore di un interesse personale e qualificato per la tutela di situazioni giuridicamente rilevanti, nonché da parte di amministrazioni, associazioni e comitati portatori di interessi pubblici o diffusi.

Per ciò che concerne le modalità di riscontro al richiedente, nel caso di esercizio del diritto di accesso ai dati, l'amministrazione é tenuta ad estrapolare dai propri archivi e documenti tutte le informazioni di carattere personale che riguardano l'interessato, riportate anche su supporto informatico, e a comunicarle a quest'ultimo in forma idonea a renderle facilmente comprensibili. A differenza dell'accesso ai documenti, l'amministrazione non pertanto é obbligata ad esibire o a consegnare copia all'interessato di atti o documenti contenenti le informazioni che lo riguardano o (eventualmente) anche dati relativi a terze persone, a meno che l'estrazione dei dati risulti particolarmente difficoltosa e le informazioni relative ai richiedenti e ai terzi siano intrecciate al tal punto da risultare incomprensibili se scomposte o private di alcuni elementi (art. 10, commi 4 e 5).

5.3. Tutela giurisdizionale.

Per quanto riguarda la tutela in sede giudiziaria del diritto di accesso ai dati personali e degli altri diritti sanciti dal Codice, la nuova disciplina prevede che «tutte le controversie riguardanti, comunque, l'applicazione delle disposizioni del Codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione» competono all'autorità giudiziaria ordinaria (art. 152).

In relazione alla tutela in sede giudiziaria del diritto di accesso agli atti amministrativi, la legge n. 241/1990 ha disposto, invece, all'art. 25, comma 5, che contro le determinazioni amministrative concernenti il diritto di accesso e nei casi di rifiuto, espresso o tacito, o di differimento dell'accesso é dato ricorso, nel termine di trenta giorni, al Tribunale amministrativo regionale.

Al riguardo é emerso un indirizzo nella giurisprudenza amministrativa, in via generale condiviso anche dalla Corte di Cassazione (si veda Cassazione civile, sez. un., 28 maggio 1998, n. 5292), in base al quale si deve riconoscere l'esistenza di una giurisdizione esclusiva amministrativa per quanto riguarda le valutazioni di legittimità degli atti amministrativi che decidono sulla richiesta di accesso, a prescindere dalla consistenza della posizione giuridica fatta valere e ciò anche nei casi in cui l'amministrazione, nel perseguire i propri interessi abbia agito quale soggetto di diritto privato (si veda Consiglio di Stato, sez. IV, 3 agosto 1995, n. 589).

6. Tematiche di interesse in materia di gestione del personale.

Com'é noto poiché la pubblica amministrazione si caratterizza per essere una organizzazione produttiva basata sul lavoro, la gestione delle risorse umane, fra le attività da essa compiute, riveste un ruolo essenziale che si interseca con la potestà organizzativa attribuita alle amministrazioni. In tale ambito, occorre porre una particolare attenzione ai principi posti dal Codice.

I profili relativi alla tutela della riservatezza sono ben noti alle pubbliche amministrazioni ed in particolare agli uffici cui compete la gestione del personale. Questi ultimi detengono ed acquisiscono un numero elevato di informazioni relative ai dipendenti dell'amministrazione. Da ciò deriva la necessità di una preliminare ricognizione delle proprie attività alla luce delle norme vigenti che deve essere costantemente aggiornata. Al riguardo, vale la pena di ricordare alcuni dei problemi emersi in questi ultimi anni ed evidenziati in diverse occasioni dal Garante.

Dal momento che le pubbliche amministrazioni raccolgono, sempre più spesso attraverso tecnologie informatiche, un numero rilevante di dati, sia in relazione ai compiti di istituto, sia in relazione alla gestione del personale dipendente (per tutte le fasi relative al rapporto di lavoro, dall'accesso all'estinzione), occorre rammentare in primo luogo che la configurazione e la gestione di queste banche dati deve essere realizzata

nel rispetto del principio di necessità sancito dall'art. 3 del Codice (v. più diffusamente supra la parte relativa ai «Principi e gli obblighi»).

In via generale, nel titolo VIII della Parte II del Codice, intitolato «Lavoro e previdenza sociale», l'art. 112, considera di rilevante interesse pubblico una serie di trattamenti di dati sensibili e giudiziari attinenti ai lavoratori e finalizzati all'instaurazione e alla gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato. Tra tali trattamenti sono compresi, in particolare, quelli effettuati al fine di accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, o la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio (art. 112, comma 2, lettera c), di adempiere agli obblighi connessi alla definizione dello stato giuridico ed economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili (lettera d), di adempiere a specifici obblighi o compiti previsti in materia di igiene e sicurezza del lavoro (lettera e), di svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile dei dipendenti (lettera g).

In particolare, in tema di <u>pubblicazione di graduatorie</u> delle procedure di selezione del personale, si sottolinea la necessità di verificare che le indicazioni contenute nelle graduatorie non comportino la divulgazione di dati idonei a rivelare lo stato di salute e di utilizzare, piuttosto, diciture generiche o codici numerici, in modo da non incorrere nel divieto di diffondere i dati attinenti alla salute sancito dall'art. 22, comma 8, del Codice.

Analoghe cautele devono essere adottate nella redazione di graduatorie relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti o abilitazioni. L'inserimento in tali atti, destinati alla pubblicazione, di informazioni riguardanti lo stato di salute degli iscritti (ad esempio relative allo stato di disabilità di un componente il nucleo familiare di uno dei beneficiari) contrasta, infatti, con la disciplina sulla protezione dei dati personali che vieta ai soggetti pubblici, autorizzati

a concedere specifici benefici connessi all'invalidità civile, di diffondere i dati relativi allo stato di salute dei soggetti beneficiari (art. 68 del Codice). L'adozione di tali accorgimenti, peraltro, non deve pregiudicare la possibilità per le persone a ciò legittimate di accedere ad eventuali altre informazioni relative agli iscritti in graduatoria, anche sensibili, in conformità alle leggi e ai regolamenti in materia di accesso alla documentazione amministrativa.

Un altro aspetto che, oltre ad impegnare particolarmente le amministrazioni, ha suscitato alcuni interventi giurisprudenziali, riguarda le richieste di accesso agli elaborati concorsuali. Sul punto si rimanda, più in generale, alla parte successiva nella quale si richiamano gli attuali orientamenti giurisprudenziali in tema di diritto di accesso agli atti detenuti dalle pubbliche amministrazioni.

Sul versante della gestione dei dati personali dei dipendenti molti sono gli aspetti di rilievo. Per quanto concerne i dati contenuti nei fascicoli personali, il Garante ha avuto modo in alcune occasioni di sottolineare che **le certificazioni mediche rese a giustificazione di assenze per malattia devono contenere soltanto la prognosi e non la diagnosi relativa alla patologia sofferta dal lavoratore.**

L'amministrazione, che non é legittimata a trattare questi dati, deve quindi adoperarsi **per oscurare le diagnosi eventualmente riportate su certificati medici già detenuti ed adottare opportuni accorgimenti anche verso lavoratori e medici affinché vengano prodotti soltanto certificati dai quali risulti la sussistenza e la durata dello stato di incapacità del lavoratore, senza alcuna indicazione diagnostica.**

Inoltre l'art. 113 del Codice richiama il disposto dell'art. 8 della legge 20 maggio 1970, n. 300, il quale stabilisce che «é fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore».

Altro tema di grande attualità é quello della vigilanza sulle comunicazioni elettroniche e sull'utilizzo di Internet sul posto di lavoro rispetto al quale si richiama il documento di lavoro delle autorità europee di protezione dei

dati riunite nel Gruppo dei Garanti europei, istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, adottato il 29 maggio 2002 (1), nonché la giurisprudenza della Corte europea dei diritti dell'uomo relativa all'art. 8 della Convenzione europea dei diritti dell'uomo.

Riguardo al tema del controllo dei lavoratori, occorre rammentare il divieto di controllo a distanza dell'attività lavorativa e le altre garanzie previste in materia di lavoro dall'art. 4 della legge n. 300/1970 richiamato dal Codice. Tali garanzie devono essere rispettate, in particolare, nel caso di installazione nei locali dell'amministrazione di impianti di videosorveglianza per motivi di sicurezza o per esigenze organizzative e dei processi produttivi, tenendo presente l'obbligo di informare, anche con formule sintetiche, i dipendenti ed i visitatori che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione (art. 13 del Codice).

Sulla specifica questione si ricordano gli indirizzi formulati dal Gruppo dei Garanti europei, nel parere dell'11 febbraio 2004, n. 4, sul trattamento dei dati personali tramite videosorveglianza (2) e il provvedimento del 29 aprile 2004 del Garante con cui sono state indicate le condizioni di liceità della installazione di sistemi di videosorveglianza. In particolare, **l'Autorità ha ribadito che i soggetti pubblici possono attivare sistemi di videosorveglianza solo in quanto siano strumentali allo svolgimento delle loro funzioni istituzionali e ha affermato che tale installazione é lecita solo se é proporzionata agli scopi che si intendono perseguire** (art. 11, comma 1, lettera d) del Codice), essendo altre misure realmente insufficienti e inattuabili (ad esempio, sistemi d'allarme o misure di protezione agli ingressi).

Al riguardo, occorre altresì valutare se sia realmente necessario raccogliere immagini dettagliate, definendo di conseguenza la dislocazione e la tipologia delle apparecchiature da installare (fisse o mobili), e limitare rigorosamente la creazione di banche dati quando, per le finalità perseguite, é sufficiente installare un sistema a circuito chiuso di sola visione delle immagini senza registrazione (ad esempio, per il controllo del flusso ad uno sportello). In armonia con il principio di necessità sancito dal Codice (art. 3), attraverso tali sistemi é poi possibile riprendere persone identificabili soltanto se, per raggiungere gli scopi prefissati, non

possono essere utilizzati dati anonimi. I cittadini che transitano nelle aree sorvegliate devono inoltre essere informati della rilevazione dei dati (art. 13 del Codice). In proposito, si rammenta che con il provvedimento citato il Garante ha messo a disposizione un modello semplificato di informativa, la quale deve essere chiaramente visibile ed indicare chi effettua la rilevazione delle immagini e per quali scopi.

Infine, sulla base dell'art. 111 del Codice, é prevista l'adozione, attraverso un procedimento che coinvolgerà le categorie interessate, di un codice di deontologia e buona condotta relativo al trattamento dei dati personali in materia di gestione del rapporto di lavoro. Le disposizioni del codice deontologico una volta pubblicate nella Gazzetta Ufficiale a cura del Garante, previa verifica della loro conformità alle leggi e ai regolamenti, acquisiranno efficacia giuridica vincolante, poiché il loro rispetto costituirà «condizione essenziale per la liceità e correttezza del trattamento dei dati personali» effettuato anche da parte dei soggetti pubblici nell'ambito della gestione del rapporto di lavoro (art. 12 del Codice).

7. L'accesso agli atti amministrativi e la tutela della riservatezza: Il contemperamento degli interessi e gli orientamenti giurisprudenziali.

Come noto il problema di fondo relativo all'applicabilità della normativa sulla tutela della riservatezza alle pubbliche amministrazioni é basato sulla possibile contrapposizione fra il principio della trasparenza dell'azione amministrativa, e quindi della pubblicità e conoscibilità degli atti delle pubbliche amministrazioni, sancito dalla legge n. 241/1990, ed il principio della tutela della riservatezza. Entrambi i principi derivano dalla Carta costituzionale essendo rispettivamente espressione dell'imparzialità e del buon andamento e della tutela dei diritti inviolabili della persona. Tali principi assumono una rilevanza assoluta per le pubbliche amministrazioni, poiché le norme che ne hanno dato attuazione concreta hanno permeato profondamente e diretto incisivamente l'attività amministrativa.

Nell'impianto della legge n. 241/1990 la tutela della riservatezza costituisce un limite al diritto di accesso (si veda l'art. 24, comma 2,

lettera d), quale eccezione alla regola della accessibilità agli atti amministrativi. Tale intendimento é stato successivamente riconfermato dal decreto del Presidente della Repubblica 27 giugno 1992, n. 352, recante il regolamento sulla disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, nel quale si prevede che l'interessato possa avere visione degli atti relativi al procedimento amministrativo quando ciò sia necessario per curare e difendere i propri interessi giuridici.

Negli anni successivi il dibattito si é dipanato intorno al tema della comparazione dei valori contrapposti, articolandosi essenzialmente sulla contrapposizione fra tutela del diritto alla riservatezza da un lato e tutela del diritto di accesso ai documenti per la difesa di un interesse giuridicamente rilevante.

La possibilità che i regolamenti di delegificazione, ai quali la legge n. 241/1990 aveva demandato la disciplina dei limiti oggettivi all'esercizio del diritto di accesso, fornissero elementi efficacemente dirimenti, non si é verificata, poiché questi si sono limitati, essenzialmente, ad indicare i documenti sottratti all'accesso.

Le amministrazioni, pertanto, per lungo tempo si sono trovate nella situazione di dover valutare caso per caso quale fosse l'esigenza prevalente, di fatto svolgendo una funzione di composizione degli interessi.

Alcuni punti di riferimento sono stati elaborati, soprattutto, dalla giurisprudenza del Consiglio di Stato, il quale ha sempre ritenuto che dovesse sempre soccorrere la disciplina legislativa (si veda ad esempio Consiglio di Stato, sez. V, 5 maggio 1999, n. 518).

L'Adunanza plenaria del Consiglio di Stato, con la decisione n. 5 del 4 febbraio 1997, in linea con lo spirito della disciplina sulla trasparenza amministrativa, ha affermato che tale disciplina accorda prevalenza al principio di pubblicità rispetto a quello di tutela della riservatezza, consentendo l'accesso anche nei confronti di documenti contenenti dati riservati, sempre che l'istanza ostensiva sia sorretta dalla necessità di difendere i propri interessi giuridici e con il limite modale della sola

visione, non essendo percorribile la modalità più penetrante e potenzialmente lesiva dell'estrazione di copia.

Con riferimento, invece, all'accesso a documenti amministrativi contenenti dati sensibili, il decreto legislativo 11 maggio 1999, n. 135, integrando la normativa sul trattamento di questi dati da parte dei soggetti pubblici (art. 16), aveva già colmato il vuoto normativo determinato dall'assenza di una espressa previsione legislativa relativa all'accesso a documenti contenenti informazioni sensibili.

Rispetto alla normativa previgente, il Codice conferma la compatibilità delle disposizioni sull'accesso ai documenti amministrativi con quelle in materia protezione dei dati personali, stabilendo che i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali e la relativa tutela giurisdizionale, restano disciplinati dalla legge n. 241/1990 e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso (art. 59). La nuova disciplina, inoltre, riproduce la previsione già contenuta nell'art. 16 del decreto legislativo n. 135/1999, in materia di trattamenti di dati sensibili da parte di soggetti pubblici, considerando le attività finalizzate all'applicazione della disciplina in materia di accesso ai documenti amministrativi di rilevante interesse pubblico.

Per ciò che concerne i limiti al diritto di accesso, nel caso in cui i documenti amministrativi oggetto della richiesta di accesso contengono dati attinenti la salute e la vita sessuale, il Codice, risolvendo alcuni dubbi interpretativi sorti sulla base del citato art. 16 del decreto legislativo n. 135/1999 ed in linea con l'orientamento interpretativo espresso al riguardo dalla giurisprudenza amministrativa (C.d.S., sez. VI, n. 1882/2001), dispone che il trattamento dei dati sensibili finalizzato a permettere l'accesso é consentito soltanto se la situazione giuridica che si intende tutelare con la richiesta di accesso é «di rango almeno pari ai diritti dell'interessato», ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile (art. 60).

In proposito il Consiglio di Stato ha sostenuto che tale valutazione deve essere fatta in concreto «in modo da evitare il rischio di soluzioni precostituite poggianti su una astratta scala gerarchica dei diritti in

contesa» (C.d.S. Sez. VI, 30 marzo 2001, n. 1882 e 9 maggio 2002, n. 2542; cfr. anche C.d.S. Sez. V, 31 dicembre 2003, n. 9276). (3)

Con il provvedimento del 9 luglio 2003, il Garante ha affrontato la questione, riferendosi in particolare alle richieste di accesso a cartelle cliniche, ma fornendo indicazioni utili anche per altri tipi di documenti detenuti in ambito pubblico, la cui ostensibilità a persone diverse dall'interessato impone comunque una valutazione sul rango dei diversi diritti coinvolti da parte dell'amministrazione destinataria della richiesta di accesso.

In tale provvedimento, l'Autorità ha precisato, in particolare, che occorre avere presente, quale elemento di raffronto per il bilanciamento degli interessi, non già il diritto alla tutela giurisdizionale, che pure é costituzionalmente garantito, bensì il diritto soggettivo sottostante, che si intende far valere sulla base del materiale documentale di cui si vorrebbe avere conoscenza. La comunicazione di dati che rientrano nella sfera di riservatezza dell'interessato può ritenersi giustificata e legittima solo se il diritto del richiedente rientra nella categoria dei diritti della personalità o é compreso tra altri diritti fondamentali ed inviolabili.

Per ciò che riguarda invece l'accesso agli elaborati concorsuali, si rammenta che la giurisprudenza amministrativa propende per la tesi favorevole all'accesso. Ciò in considerazione del fatto che, essendo gli elaborati concorsuali, per loro natura destinati ad una valutazione e ad una comparazione, la riservatezza delle prove non può essere ritenuta prevalente rispetto all'esigenza di difesa di interessi giuridici. Pertanto il diritto all'accesso può essere fatto valere anche prima che si verifichi una lesione concreta e si esplica fino al diritto ad avere copia degli elaborati e dei titoli degli altri candidati (si vedano Consiglio di Stato, sez. IV, 13 gennaio 1995, n. 5; Consiglio di Stato, sez. VI, 13 settembre 1996, n. 1221). Più recentemente la giurisprudenza amministrativa ha affermato un principio di maggiore cautela, cioé quello della, pertinenza, in base al quale l'accesso agli atti di una procedura concorsuale deve essere consentito, previa garanzia dell'anonimato degli altri concorrenti, in relazione alle stesse prove sostenute dal richiedente (si veda TAR Toscana, sez. I, 9 marzo 1999, n. 146).

Le amministrazioni avvieranno tutte le iniziative di informazione e formazione dirette ad accrescere la conoscenza del Codice e della presente direttiva al fine di favorire, in particolare, l'attuazione delle regole per il trattamento dei dati personali, sensibili e giudiziari.

I Ministeri provvederanno a sollecitare le amministrazioni da esse vigilate perché predispongano, nei termini previsti, gli atti regolamentari di cui agli articoli 20, comma 2, e 21, comma 2, del Codice.

La presente direttiva é inviata all'Ispettorato per la funzione pubblica al quale é demandata dall'ordinamento l'attività di vigilanza e verifica dell'attuazione e corretta applicazione delle riforme amministrative, con particolare riferimento alle innovazioni più significative in tema di rapporti tra cittadini e amministrazioni pubbliche, secondo quanto previsto dal decreto sull'organizzazione interna del Dipartimento della funzione pubblica in corso di pubblicazione.

Roma, 11 febbraio 2005

Il Ministro per la funzione pubblica: Baccini

Registrata alla Corte dei conti il 4 aprile 2005

Ministeri istituzionali, Presidenza del Consiglio dei Ministri, registro n. 4, foglio n. 224

(1) Reperibile all'indirizzo: http://www.europa.eu.int/comm/internal market/privacy/workingroup/wp 2002/wpdocs02 en.htm

(2) Reperibile all'indirizzo: http://www.europa.eu.int/comm/internal market/privacy/workingroup/wp 2004/wpdocs04 en.htm

(3) Su questa linea interpretativa si é mossa la giurisprudenza successiva (cfr. ad es. TAR Lazio, sez. Latina, 15 novembre 2002, n. 1179; TAR Abruzzo, sez. Pescara, 14 giugno 2002, n. 533; TAR Lazio, 8 marzo 2004, n. 4874; TAR Liguria, 26 febbraio 2004, n. 414).

Privacy e pubblico impiego: le "Linee guida" del Garante

Sul sito web del *"Garante per la protezione dei dati personali"* sono pubblicate le *"**Linee guida**"* in materia di trattamento di detti dati concernenti i lavoratori pubblici, per finalità di gestione del rapporto di lavoro (deliberazione n. 23 del 14.6.2007).

Le *"Linee guida"* in questione seguono quelle per il trattamento dei dati relativi ai dipendenti privati *(G.U. n. 285 del 7.12.2006)*.

Di seguito, in sintesi, alcuni dei punti principali del provvedimento in corso di pubblicazione nella Gazzetta Ufficiale.

*** * ***La **premessa** individua lo scopo delle *"Linee guida"* e gli ambiti di intervento, fornendo indicazioni e raccomandazioni riguardo al trattamento dei dati personali.

*** * ***Il **paragrafo 2** affronta **il rispetto dei principi di protezione dei dati personali** coniugandolo con il diritto alla trasparenza.

Il rispetto di tali principi, pertanto, non esclude il trattamento lecito di dati personali per finalità, ad esempio, di tipo sindacale.

Oltre alle leggi e ai regolamenti, anche i contratti collettivi (nazionali ed integrativi) contengono alcune previsioni che permettono di trattare lecitamente informazioni di natura personale per ciò che riguarda l'attività sindacale.

Viene raccomandato, in tal senso, di porre attenzione alle disposizioni dei contratti collettivi che prevedono la conoscenza di

dati da parte di organizzazioni sindacali: bisogna discernere adeguatamente affinché il doveroso rispetto degli obblighi di informativa, consultazione, concertazione e contrattazione - da cui deriva la comunicazione delle informazioni alle organizzazioni sindacali - avvenga nel rispetto dei principi di necessità e di proporzionalità del trattamento dei dati.

In tale ottica e nell'ambito della disciplina contrattuale, si suggerisce di prevedere un accesso preliminare del sindacato a dati aggregati (riferiti cioè all'intera struttura lavorativa o a singole unità oppure a gruppi di lavoratori) e in un secondo momento, in caso di successive anomalie o di particolari esigenze di verifica, consentire all'organizzazione sindacale - ma solo nei casi espressamente previsti e circostanziati - di conoscere anche informazioni personali relative a singoli o a gruppi di lavoratori.

Ciò semprechè sia effettivamente necessario al fine di dimostrare la corretta applicazione delle clausole pattuite in sede di contrattazione e la comunicazione sia limitata alle sole informazioni pertinenti e mai eccedenti lo scopo.

*** * ***Nel **paragrafo 3** si ribadisce in modo puntuale l'importanza della corretta individuazione delle figure - **titolare, responsabile e incaricati del trattamento** - riferite alle amministrazioni più articolate; un paragrafo specifico è dedicato al medico competente.

*** * *Dati sensibili e rapporto di lavoro** sono l'oggetto del **paragrafo 4** che richiama la responsabilità del datore di lavoro pubblico a limitare il trattamento dei dati sensibili e giudiziari alle sole informazioni e operazioni individuate e rese pubbliche con lo specifico atto regolamentare previsto dal *Codice Privacy* (artt. 20, 21, 112 e 154) che doveva essere adottato entro il termine transitorio del 28.2.2007.

La mancata adozione di tale schema regolamentare produce l'immediata illiceità ed inutilizzabilità dei dati trattati dalla pubblica amministrazione; è prevista, inoltre, l'adozione di provvedimenti giudiziari di blocco o di divieto del trattamento.

Resta ferma, comunque, per le amministrazioni pubbliche la possibilità di provvedere con sollecitudine ad adottare il regolamento suddetto - nel caso non lo abbiano fatto entro il termine stabilito - al fine di dare la *"veste"* di legittimità ai dati sensibili e giudiziari in corso di trattamento.

*** * ***

Ampio spazio viene dato alle modalità di **comunicazione di dati personali***,* descritte nel **paragrafo 5.** In tal caso l'amministrazione è tenuta ad adottare con il dipendente forme di comunicazione protette ed individualizzate: inoltrando le note in busta chiusa o inviandole all'e-mail personale ovvero invitandolo a ritirare personalmente la documentazione.

In questo ambito trovano soluzione i rapporti con le organizzazioni sindacali e il loro diritto di informazione.

Un sottoparagrafo, infatti, è dedicato espressamente ai **rapporti con le organizzazioni sindacali:** in questa sede sono riprese le considerazioni già svolte nel primo paragrafo, a proposito del trattamento dei dati personali, per declinarle in chiave di relazioni sindacali*.*

Sulla base delle disposizioni dei contratti collettivi, sono oggetto di specifici diritti di informazione sindacale preventiva o successiva i criteri generali e talune modalità di gestione del rapporto di lavoro.

Ad esclusione dei casi in cui il contratto collettivo preveda espressamente che l'informativa sindacale abbia ad oggetto anche dati nominativi del personale al fine di poter verificare la corretta attuazione di determinati atti di natura organizzativa (e il contratto scuola risulta tra questi, come specificato nella nota 19 della delibera, consentendo, quindi, l'accesso ai dati individuali), l'amministrazione può fornire alle organizzazioni sindacali dati numerici o aggregati ma non quelli riferibili ad uno o più lavoratori individuabili.

Resta, tuttavia, disponibile per l'organizzazione sindacale anche la possibilità di presentare istanze di accesso a dati personali attinenti ad uno o più lavoratori su delega o procura, come pure la facoltà di esercitare il diritto di accesso a documenti amministrativi in materia di gestione del personale, nel rispetto delle condizioni, dei limiti e delle modalità previsti dalle norme vigenti, e per salvaguardare un interesse giuridicamente rilevante di cui sia portatore il medesimo sindacato.

Il rifiuto, anche tacito, dell'accesso ai documenti amministrativi, è suscettibile di impugnativa presso l'autorità giudiziaria, la Commissione per l'accesso o il difensore civico.

L'amministrazione può anche rendere note alle organizzazioni sindacali informazioni personali relative alle ritenute effettuate a carico dei relativi iscritti.

* * *

Il **paragrafo 6** è dedicato alla **diffusione via internet e/o cartacea di dati personali**. Nelle graduatorie relative a concorsi o selezioni vanno riportati solo dati pertinenti (elenchi nominativi abbinati ai risultati, elenchi di ammessi alle prove scritte o orali; non è lecito riportare tipologie di informazione non pertinenti, quali, recapiti di telefonia fissa o mobile o il codice fiscale).

Se i dati sono diffusi tramite *internet* le amministrazioni devono assicurare l'esattezza, l'aggiornamento e la pertinenza dei dati pubblicati in rete e garantire il *"diritto all'oblio"* (trascorso un certo periodo di tempo dalla pubblicazione è opportuno spostare i nominativi in una parte del sito dove non siano più rintracciabili da motori di ricerca esterni).

Nell'ambito della diffusione dei dati personali, il Garante ha osservato come, relativamente all'organizzazione degli uffici pubblici, alcuni specifici obblighi normativi impongono alle amministrazioni di rendere noti, attraverso i propri siti internet, determinati dati personali concernenti i propri dipendenti (ad es. l'organigramma degli uffici e l'elenco delle caselle di posta elettronica, utilizzabili - naturalmente - per soli scopi istituzionali).

Salvo ipotesi specifiche, espressamente previste da disposizioni di legge, non è lecito di norma diffondere informazioni personali riferite a singoli lavoratori pubblicando, con documenti interni affissi nei luoghi di lavoro o con atti e/o circolari destinati alla collettività dei lavoratori (come nell'ipotesi di informazioni riguardanti contratti individuali di lavoro) trattamenti stipendiali o accessori percepiti, assenze dal lavoro per malattia, ferie, permessi, iscrizione/adesioni di singoli dipendenti ad associazioni.

Nel caso dei c.d. cartellini identificativi, le amministrazioni, nel selezionare i dati personali destinati alla diffusione tramite il cartellino, sono tenute a rispettare il principio della pertinenza e della non eccedenza dei dati in rapporto alle finalità perseguite.

* * *

Il **paragrafo 7** tratta di **dati biometrici** dei lavoratori pubblici. Anche nell'ambito pubblico non è consentito un uso generalizzato dei dati biometrici dei dipendenti (impronte digitali, iride); per controllare le presenze o gli accessi sul luogo di lavoro il Garante può autorizzare tali sistemi solo in caso di particolari esigenze.

* * *

Il **paragrafo 8** è dedicato ai dati **idonei a rivelare lo stato di salute**. I certificati medici da presentare in caso di assenza per malattia vanno consegnati con la sola *prognosi,* vale a dire la data iniziale e quella finale della presunta durata dell'assenza. Si esclude, espressamente, che il datore di lavoro pubblico debba venire a conoscenza di dati relativi alla *diagnosi*. Ciò vale anche con riferimento alle visite fiscali di controllo.

In caso di visite medico-legali, i collegi medici devono trasmettere all'amministrazione di appartenenza dell'interessato il relativo verbale di visita con la sola indicazione del giudizio medico-legale di idoneità, inidoneità o altre forme di inabilità.

Nel caso di lavoratore che beneficia dei permessi di cui alla legge 104/92 relativamente ad un familiare, l'amministrazione di appartenenza non deve venire a conoscenza di dati personali del congiunto portatore di handicap relativi alla diagnosi o all'anamnesi accertate dalla commissione medica, bensì della certificazione dalla quale risulti esclusivamente l'accertata condizione di handicap grave per opera dell'apposito collegio medico.

Diversamente, per fruire di permessi o congedi per gravi infermità o altri gravi motivi familiari, il lavoratore è tenuto per legge a produrre alla propria amministrazione idonea documentazione medica attestante le gravi infermità o le gravi patologie da cui risultino affetti i propri familiari.

Allo stesso modo il datore di lavoro pubblico può venire a conoscenza dello stato di tossicodipendenza di un proprio dipendente o di un familiare di questi, in caso di richieste di accesso o concorso a programmi riabilitativi o terapeutici con conservazione del posto di lavoro (senza retribuzione), atteso l'onere di presentare specifica documentazione medica al proprio datore di lavoro.

*** * ***

Il **paragrafo 9**, infine, si occupa dei dati **idonei a rilevare le convinzioni religiose** e delle cautele da osservare nel trattamento di tali tipologie di dati sensibili.

"Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" - 14 giugno 2007
(G.U. 13 luglio 2007, n. 161)

Registro delle deliberazioni
Deliberazione n. 23
del 14 giugno 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), anche in riferimento all'art. 154, comma 1, lett. h);

Esaminate le istanze (segnalazioni e quesiti) pervenute riguardo al trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico;

Ritenuta l'opportunità di individuare un quadro unitario di misure e di accorgimenti necessari e opportuni, volti a fornire orientamenti utili per cittadini e amministrazioni interessate;

Visto il testo unico delle leggi sull'ordinamento degli enti locali (d.lg. 18 agosto 2000, n. 267);

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il dott. Mauro Paissan;

DELIBERA:

1. di adottare le *"Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico"* contenute nel documento allegato quale parte integrante della presente deliberazione (Allegato 1);

2. che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 14 giugno 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico

(Deliberazione n. 23 del 14 giugno 2007)

Sommario

1. Premessa

1.1. **Scopo delle linee guida**. Per fornire indicazioni e raccomandazioni riguardo alle operazioni di trattamento effettuate con dati personali (anche sensibili) di lavoratori alle dipendenze di datori di lavoro pubblici, il Garante ravvisa l'esigenza di adottare le presenti linee guida, suscettibili di periodico aggiornamento, nelle quali si tiene conto di precedenti decisioni dell'Autorità.

Le presenti linee guida seguono quelle adottate rispetto agli analoghi trattamenti effettuati da datori di lavoro privati [(1)], con le quali coincidono per molteplici aspetti che sono comunque riprodotti nel presente documento.

L'adozione di distinte linee guida per il settore pubblico deriva dall'esigenza di evidenziare, nel quadro della tendenziale uniformità dei princìpi applicabili al rapporto di lavoro [(2)], alcune specificità che si pongono per i soggetti pubblici datori di lavoro (taluni presupposti del trattamento; speciali disposizioni che prevedono casi di necessaria comunicazione o diffusione di dati; situazioni particolari).

Come per il settore privato, le indicazioni fornite non pregiudicano l'applicazione delle disposizioni di legge o di regolamento che stabiliscono particolari divieti o limiti in relazione a taluni settori o a specifici casi di trattamento (artt. 113, 114 e 184, comma 3, del Codice).

1.2. **Ambiti considerati.** Le tematiche prese in considerazione si riferiscono, in particolare, alla comunicazione e alla diffusione di dati e al trattamento delle informazioni sensibili (in specie, di quelli idonei a rivelare lo stato di salute e le convinzioni religiose) o di dati biometrici relativi a lavoratori alle dipendenze di pubbliche amministrazioni.

2. Il rispetto dei princìpi di protezione dei dati personali

2.1. **Considerazioni generali**. Anche per i datori di lavoro pubblici il trattamento dei dati personali è disciplinato assicurando un livello elevato di tutela dei diritti e delle libertà fondamentali e conformando il medesimo trattamento ai princìpi di semplificazione, armonizzazione ed efficacia, sia per le modalità di esercizio dei diritti, sia per l'adempimento degli obblighi da parte dei titolari del trattamento [(3)].

I lavoratori, nel rapporto con il proprio datore di lavoro pubblico, hanno diritto di ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei predetti diritti e libertà [(4)].

Assume quindi particolare rilievo la necessità che i soggetti pubblici colgano l'occasione della progressiva introduzione di nuove tecniche rispetto alle modalità tradizionali di trattamento dei dati su base cartacea per valutare preventivamente come rendere efficienti i propri sistemi informativi, individuando forme adeguate di trattamento che tutelino appieno i lavoratori.

Le cautele e gli accorgimenti devono essere opportunamente graduati tenendo conto anche delle diverse forme del trattamento e della differente natura dei dati comuni e sensibili.

2.2. **Liceità, pertinenza, trasparenza.** Il datore di lavoro pubblico può lecitamente trattare dati personali dei lavoratori nella misura in cui ciò sia necessario per la corretta gestione del rapporto di lavoro, avendo cura di applicare le previsioni che riguardano le proprie funzioni istituzionali o il rapporto di lavoro, contenute in leggi, regolamenti, contratti e in accordi collettivi, in modo da avvalersi di informazioni personali e modalità di trattamento proporzionate ai singoli scopi.

Il Codice in materia di protezione dei dati personali, anche in attuazione di direttive comunitarie (nn. 95/46/Ce e 2002/58/Ce), prescrive che il trattamento di dati personali per la gestione del rapporto di lavoro avvenga, in particolare:

- rispettando i princìpi di necessità, di liceità e di qualità dei dati (artt. 3 e 11 del Codice);
- attenendosi alle funzioni istituzionali e applicando i presupposti e i limiti previsti da leggi e regolamenti rilevanti per il trattamento, in particolare in materia di pubblico impiego (art. 18 del Codice);
- dando applicazione effettiva e concreta al principio di indispensabilità nel trattamento dei dati sensibili e giudiziari, il quale vieta di trattare informazioni o di effettuare operazioni che non siano realmente indispensabili per raggiungere determinate finalità previste specificamente (artt. 4, comma 1, lett. d) ed e), 22, commi 3, 5 e 9, e 112 del Codice);
- limitando il trattamento di dati sensibili e giudiziari alle sole informazioni ed operazioni di trattamento individuate e rese pubbliche con l'atto regolamentare adottato in conformità al parere del Garante (artt. 20, 21, 112 e 154 del Codice);
- informando preventivamente e adeguatamente gli interessati (art. 13 del Codice);
- adottando adeguate misure di sicurezza, idonee a preservare i dati da alcuni eventi tra cui accessi ed utilizzazioni indebiti, rispetto ai quali l'amministrazione può essere chiamata a rispondere anche civilmente e penalmente (artt. 15 e 31 e ss. del Codice).

2.3. **Finalità.** Il trattamento dei dati personali, anche sensibili, riferibili ai lavoratori deve essere orientato in concreto all'esclusivo o prevalente scopo di adempiere agli obblighi e ai compiti in materia di rapporto di lavoro e di impiego alle dipendenze delle amministrazioni pubbliche.

Oltre alle leggi e ai regolamenti, anche i contratti collettivi (nazionali e integrativi) contengono alcune previsioni che permettono di trattare lecitamente informazioni di natura personale anche per ciò che attiene all'attività sindacale (ad esempio, per determinare il trattamento economico fondamentale ed accessorio, per fruire di permessi o di aspettative sindacali, per accedere a qualifiche, per la mobilità o per la responsabilità disciplinare).

Il trattamento effettuato dal soggetto pubblico deve attenersi in concreto a queste disposizioni e restare compatibile con le finalità per le quali i dati sono stati inizialmente raccolti o già trattati (art. 11, comma 1, lett. b), del Codice).

Particolare attenzione deve essere posta alle disposizioni dei contratti collettivi che prevedono la conoscenza di dati da parte di organizzazioni sindacali, avendo cura che il doveroso rispetto degli obblighi di informativa, consultazione, concertazione e contrattazione che comportano la comunicazione di informazioni alle medesime organizzazioni avvenga nel rispetto dei princìpi di necessità e proporzionalità.

I soggetti pubblici potrebbero peraltro cogliere l'occasione dei rinnovi dei contratti collettivi per verificare l'attualità e la chiarezza di tali previsioni contrattuali, verificando anche la loro adeguatezza rispetto a casi che si verificano in concreto (si pensi al problema della contestuale iscrizione dei lavoratori a più organizzazioni sindacali contestata da alcuna di esse).

In questo quadro occorre anche mantenere distinti i casi in cui è prevista specificamente la comunicazione solo di dati numerici aggregati da quelli in cui, in un'ottica di trasparenza e graduazione dell'accesso delle organizzazioni sindacali ad informazioni personali che risultino necessarie per verificare in conformità alla legge la concreta applicazione delle disposizioni del contratto collettivo da parte del datore di lavoro, è invece consentita (ed è giustificata in

rapporto al caso concreto) la conoscenza di dati riferiti a singoli lavoratori.

In tale ottica, nell'ambito della disciplina contrattuale, si potrebbe pertanto prevedere di regola un accesso preliminare del sindacato a dati aggregati, riferiti all'intera struttura lavorativa o a singole unità organizzative ovvero a gruppi di lavoratori e, soltanto in presenza di successive anomalie o di specifiche esigenze di verifica, consentire (in casi espressamente previsti e circostanziati) all'organizzazione sindacale di conoscere anche informazioni personali relative a singoli o a gruppi di lavoratori. Ciò sempreché, nel caso concreto, sia effettivamente necessario per dimostrare la corretta applicazione dei criteri pattuiti e la comunicazione sia limitata alle informazioni pertinenti e non eccedenti rispetto a tale scopo. Resta fermo che l'eventuale successivo trattamento illecito o non corretto delle informazioni acquisite da parte dell'organizzazione sindacale si svolge nella sfera di responsabilità della medesima organizzazione [(5)].

3. Titolare, responsabile e incaricati del trattamento

3.1. **Corretta individuazione delle figure.** Resta importante individuare correttamente i soggetti che, a diverso titolo, possono trattare i dati nell'ambito della pubblica amministrazione "titolare" del trattamento ("incaricati"; eventuali "responsabili"), definendo chiaramente le rispettive attribuzioni (artt. 4, comma 1, lett. f), g) e h), 28, 29 e 30 del Codice).

Rinviando per brevità di esposizione ai numerosi pronunciamenti del Garante sul tema, giova ricordare che in linea di principio, per individuare il titolare del trattamento, occorre far riferimento all'amministrazione o ente centrale o locale nel suo complesso, anziché a singole articolazioni interne o alle persone fisiche che l'amministrano o la rappresentano (ad esempio, il ministro, il direttore generale o il presidente) [(6)].

Nelle amministrazioni più articolate, specie di grandi dimensioni o ramificate sul territorio, è possibile che alcune figure o unità organizzative siano dotate in conformità alla legge di poteri

decisionali effettivamente del tutto autonomi riguardo ai trattamenti di dati personali. In tal caso, rispettando in concreto quanto previsto dal Codice (art. 28), tali articolazioni possono essere considerate lecitamente quali "titolari" autonomi o eventuali "contitolari del trattamento" (si pensi, ad esempio, ad una singola direzione generale o area geografica di un'amministrazione ministeriale di particolare complessità organizzativa [(7)]).

Nel rispetto dei princìpi generali sopra richiamati in materia di trattamento di dati personali (cfr. punto 2), le amministrazioni devono disciplinare le modalità del trattamento, designando gli eventuali soggetti responsabili e, in ogni caso, le persone fisiche incaricate, che possono acquisire lecitamente conoscenza dei dati inerenti alla gestione del rapporto di lavoro, attenendosi alle funzioni svolte e a idonee istruzioni scritte (artt. 4, comma 1, lett. g) e h), 29 e 30).

È, infatti, facoltà delle amministrazioni designare alcuni soggetti (persone fisiche o giuridiche, enti od organismi) quali "responsabili" del trattamento, delineandone analiticamente e per iscritto i compiti attribuiti, e individuando al loro interno, se del caso, ulteriori livelli di responsabilità in base all'organizzazione delle divisioni e degli uffici o alle tipologie di trattamenti, di archivi e di dati, sempreché ciascuno di questi dimostri l'esperienza, la capacità e l'affidabilità richieste dalla legge (art. 29 del Codice).

È necessario invece che ogni lavoratore sia preposto per iscritto, in qualità di "incaricato", alle operazioni di trattamento e sia debitamente istruito in ordine all'accesso e all'utilizzo delle informazioni personali di cui può venire a conoscenza nello svolgimento della propria prestazione lavorativa. La designazione degli incaricati può essere effettuata nominativamente o, specie nell'ambito di strutture organizzative complesse, mediante atti di preposizione del lavoratore a unità organizzative per le quali venga altresì previamente individuato, per iscritto, l'ambito del trattamento consentito (art. 30 del Codice).

3.2. **Medico competente.** Anche il datore di lavoro pubblico deve svolgere alcuni trattamenti di dati in applicazione della disciplina in

materia di igiene e sicurezza del lavoro (art. 1, commi 1 e 2, d.lg. n. 626/1994 e successive modificazioni e integrazioni).

Tale disciplina, che attua anche alcune direttive comunitarie e si colloca nella cornice più ampia delle misure necessarie a tutelare l'integrità psico-fisica dei lavoratori, pone direttamente in capo al medico competente in materia di igiene e sicurezza nei luoghi di lavoro la sorveglianza sanitaria obbligatoria (e, ai sensi degli artt. 16 e 17 del d.lg. n. 626/1994, il correlato trattamento dei dati contenuti in cartelle cliniche).

In questo ambito il medico competente effettua accertamenti preventivi e periodici sui lavoratori (art. 33 d.P.R. n. 303/1956; art. 16 d.lg. n. 626/1994) e istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio (in conformità alle prescrizioni contenute negli artt. 17, 59-*quinquiesdecies*, comma 2, lett. b), 59-*sexiesdecies*, 70, 72-*undecies* e 87 d.lg. n. 626/1994).

Detta cartella è custodita presso l'amministrazione *"con salvaguardia del segreto professionale, e consegnata in copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne fa richiesta"* (artt. 4, comma 8, e 17, comma 1, lett. d), d.lg. n. 626/1994); in caso di cessazione del rapporto di lavoro le cartelle sono trasmesse all'Istituto superiore prevenzione e sicurezza sul lavoro-Ispesl (artt. 59-sexiesdecies, comma 4, 70, comma 4, 72-undecies, comma 3 e 87, comma 3, lett c), d.lg. n. 626/1994), in originale e in busta chiusa [(8)].

In relazione a tali disposizioni, al medico competente è consentito trattare dati sanitari dei lavoratori anche mediante annotazione nelle cartelle sanitarie e di rischio, e curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate. Ciò, quale che sia il titolare del trattamento effettuato a cura del medico.

Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali dell'amministrazione (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti) ma, come detto, "con salvaguardia del segreto professionale" [(9)].

Il datore di lavoro pubblico è tenuto, su parere del medico competente (o qualora quest'ultimo lo informi di anomalie imputabili all'esposizione a rischio), ad adottare le misure preventive e protettive per i lavoratori interessati; in questo specifico contesto il datore di lavoro può accedere al giudizio di idoneità del lavoratore allo svolgimento di date mansioni, anziché alle specifiche patologie accertate [(10)].

Il medico può farsi assistere da personale sanitario, anche dipendente dello stesso datore di lavoro pubblico, che deve essere designato quale incaricato del trattamento dei dati personali impartendo ad esso specifiche istruzioni per salvaguardare la segretezza delle informazioni trattate (art. 30 del Codice). In tal caso, a prescindere da quale sia il titolare del trattamento e dagli eventuali obblighi in tema di segreto d'ufficio, il medico competente deve predisporre misure idonee a garantire il rispetto del segreto professionale da parte dei propri collaboratori che non siano tenuti per legge al segreto professionale, mettendoli ad esempio a conoscenza di tali disposizioni e delle relative sanzioni (art. 10 del codice di deontologia medica del 16 dicembre 2006; art. 4 del codice deontologico per gli infermieri del maggio del 1999) [(11)].

4. Dati sensibili e rapporto di lavoro

Le pubbliche amministrazioni devono adottare maggiori cautele se le informazioni personali sono idonee a rivelare profili particolarmente delicati della vita privata dei propri dipendenti quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere e l'origine razziale ed etnica (art. 4, comma 1, lett. d), del Codice).

In linea generale il datore di lavoro pubblico può utilizzare informazioni sensibili relative al proprio personale in attuazione della normativa in materia di instaurazione e gestione di rapporti di lavoro di qualunque tipo, per finalità di formazione, nonché per concedere benefici economici e altre agevolazioni (artt. 112, 95 e 68 del Codice).

Come sopra ricordato, il datore di lavoro pubblico deve limitare il trattamento dei dati sensibili e giudiziari alle sole informazioni ed operazioni individuate e rese pubbliche con l'atto regolamentare adottato in conformità al parere del Garante (artt. 20, 21, 112 e 154 del Codice) [(12)].

Nel perseguire tali finalità occorre comunque rispettare i princìpi di necessità e di indispensabilità che impongono di ridurre al minimo l'utilizzo di dati personali e, quando non si possa prescindere dall'uso di informazioni personali sensibili o giudiziarie, di trattare dati solo in riferimento ai tipi di dati e di operazioni indispensabili in relazione alla specifica finalità di gestione del rapporto di lavoro (artt. 3 e 22 del Codice).

Scaduto il termine transitorio del 28 febbraio 2007, il trattamento da parte di un soggetto pubblico che non sia previsto da tali fonti normative è ora illecito e, oltre all'inutilizzabilità dei dati trattati, può comportare l'adozione di provvedimenti anche giudiziari di blocco o di divieto del trattamento (art. 154 del Codice; art. 3 d.l. 24 giugno 2004, n. 158, come modificato dalla l. 27 luglio 2004, n. 188; art. 11, commi 1, lett. a) e 2, del Codice) [(13)].

Resta ferma la possibilità per le amministrazioni che non abbiano eventualmente adottato i necessari atti regolamentari entro il suddetto termine, di provvedervi comunque con sollecitudine, al fine rendere leciti i trattamenti dei dati sensibili e giudiziari.

5. Comunicazione di dati personali

5.1. **Comunicazione.** Specifiche disposizioni legislative o regolamentari individuano i casi in cui l'amministrazione pubblica è legittimata a comunicare informazioni che riguardano i lavoratori a terzi, soggetti pubblici o privati (art. 19 del Codice).

Quando manca una tale previsione specifica non possono essere quindi comunicati dati personali del dipendente (ad esempio, quelli inerenti alla circostanza di un'avvenuta assunzione, allo status o alla qualifica ricoperta, all'irrogazione di sanzioni disciplinari, a trasferimenti del lavoratore come pure altre informazioni contenute

nei contratti individuali di lavoro) a terzi quali associazioni (anche di categoria), conoscenti, familiari e parenti.

Devono ritenersi in linea generale lecite le comunicazioni a terzi di informazioni di carattere sensibile relative ad uno o più dipendenti, quando esse siano realmente indispensabili per perseguire le finalità di rilevante interesse pubblico connesse all'instaurazione e alla gestione di rapporti di lavoro da parte di soggetti pubblici di cui all'art. 112 del Codice. Tali comunicazioni possono avere ad oggetto dati individuati nei pertinenti atti regolamentari dell'amministrazione e che siano in concreto indispensabili, pertinenti e non eccedenti in rapporto ai compiti e agli adempimenti che incombono al soggetto pubblico in qualità di datore di lavoro in base alla normativa sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche (artt. 20 e 22 del Codice) [(14)].

La disciplina di protezione dei dati consente inoltre al datore di lavoro pubblico di rendere conoscibili a terzi dati personali del dipendente in attuazione delle disposizioni che definiscono presupposti, modalità e limiti per l'esercizio del diritto d'accesso a documenti amministrativi (contenenti dati personali) [(15)] o che prevedono un determinato regime di conoscibilità per talune informazioni (16), ovvero in virtù di una delega conferita dall'interessato.

Oltre a designare i soggetti che possono venire lecitamente a conoscenza dei dati inerenti alla gestione del rapporto di lavoro, quali incaricati o responsabili del trattamento, il datore di lavoro deve adottare particolari cautele anche nelle trasmissioni di informazioni personali che possono intervenire tra i medesimi incaricati o responsabili nelle correnti attività di organizzazione e gestione del personale. In tali flussi di dati occorre evitare, in linea di principio, di fare superflui riferimenti puntuali a particolari condizioni personali riferite a singoli dipendenti, specie se riguardanti le condizioni di salute, selezionando le informazioni di volta in volta indispensabili, pertinenti e non eccedenti (artt. 11 e 22 del Codice) [(17)].

A tal fine, può risultare utile esplicitare delicate situazioni di disagio personale solo sulla base di espressioni generiche e utilizzando, in

casi appropriati, codici numerici, come pure riportare tali informazioni -quale presupposto degli atti adottati- solo nei provvedimenti messi a disposizione presso gli uffici per eventuali interessati e controinteressati (limitandosi quindi a richiamarli anche nelle comunicazioni interne e indicando gli estremi o un estratto del loro contenuto) [(18)].

5.2 **Rapporti con le organizzazioni sindacali.** Le pubbliche amministrazioni possono comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o a gruppi di lavoratori: si pensi al numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate nelle varie articolazioni organizzative, agli importi di trattamenti stipendiali o accessori individuati per fasce o qualifiche/livelli professionali, anche nell'ambito di singole funzioni o unità organizzative.

Sulla base delle disposizioni dei contratti collettivi, i criteri generali e le modalità inerenti a determinati profili in materia di gestione del rapporto di lavoro sono oggetto di specifici diritti di informazione sindacale preventiva o successiva.

Ad esclusione dei casi in cui il contratto collettivo applicabile preveda espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale per verificare la corretta attuazione di taluni atti organizzativi [(19)], l'amministrazione può fornire alle organizzazioni sindacali dati numerici o aggregati e non anche quelli riferibili ad uno o più lavoratori individuabili [(20)]. É il caso, ad esempio, delle informazioni inerenti ai sistemi di valutazione dell'attività dei dirigenti, alla ripartizione delle ore di straordinario e alle relative prestazioni, nonché all'erogazione dei trattamenti accessori [(21)].

Resta disponibile per l'organizzazione sindacale anche la possibilità di presentare istanze di accesso a dati personali attinenti ad uno o più lavoratori su delega o procura (art. 9, comma 2, del Codice), come pure la facoltà di esercitare il diritto d'accesso a documenti amministrativi in materia di gestione del personale, nel rispetto delle condizioni, dei limiti e delle modalità previsti dalle norme vigenti e per salvaguardare un interesse giuridicamente rilevante di cui sia portatore il medesimo sindacato (artt. 59 e 60 del

Codice) [(22)]. Il rifiuto, anche tacito, dell'accesso ai documenti amministrativi, è impugnabile presso il tribunale amministrativo regionale, la Commissione per l'accesso presso la Presidenza del Consiglio dei ministri o il difensore civico (artt. 25 e ss. l. 7 agosto 1990, n. 241; art. 6 d.P.R. 12 aprile 2006, n. 184).

L'amministrazione può anche rendere note alle organizzazioni sindacali informazioni personali relative alle ritenute effettuate a carico dei relativi iscritti, in conformità alle pertinenti disposizioni del contratto applicabile [(23)] e alle misure di sicurezza previste dal Codice (artt. 31-35).

5.3. **Modalità di comunicazione.** Fuori dei casi in cui forme e modalità di divulgazione di dati personali siano regolate specificamente da puntuali previsioni (cfr. art. 174, comma 12, del Codice), l'amministrazione deve utilizzare forme di comunicazione individualizzata con il lavoratore, adottando le misure più opportune per prevenire la conoscibilità ingiustificata di dati personali, in particolare se sensibili, da parte di soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali).

L'utilizzo del telefax come mezzo di comunicazione è consentito sebbene, in taluni casi, specifiche disposizioni prevedano apposite modalità di inoltro delle comunicazioni, come, ad esempio, nell'ambito di procedimenti disciplinari [(24)]. Anche per il telefax si devono comunque adottare opportune cautele che favoriscano la conoscenza dei documenti da parte delle sole persone a ciò legittimate.

6. Diffusione di dati personali

La diffusione di dati personali riferiti ai lavoratori può avvenire quando è prevista espressamente da disposizioni di legge o di regolamento (artt. 4, comma 1, lett. m) e 19, comma 3, del Codice), anche mediante l'uso delle tecnologie telematiche (art. 3 d.lg. 7 marzo 2005, n. 82, recante il *"Codice dell'amministrazione digitale"*).

A parte quanto eventualmente previsto sul piano normativo per specifiche categorie di atti, l'amministrazione, sulla base di apposite disposizioni regolamentari può, infatti, valorizzare anche l'utilizzo di reti telematiche per mettere a disposizione atti e documenti contenenti dati personali (es. concorsi o a selezioni pubbliche) nel rispetto dei princìpi di necessità, pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. d), del Codice).

Occorre, poi, una specifica valutazione per selezionare le informazioni eventualmente idonee a rivelare lo stato di salute degli interessati, la cui diffusione è vietata (artt. 22, comma 8, del Codice). A tale divieto non è consentito derogare invocando generiche esigenze di pubblicità connesse alla trasparenza delle procedure in materia di organizzazione del personale e degli uffici, come quelle relative alla mobilità dei dipendenti pubblici (25). Non è ad esempio consentito diffondere i nominativi degli aventi diritto al collocamento obbligatorio contenuti in elenchi e graduatorie, atteso che il divieto di diffusione dei dati idonei a rivelare lo stato di salute è ribadito espressamente dal Codice anche in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge e dai regolamenti (art. 68, comma 3, del Codice) (26).

6.1 **Dati relativi a concorsi e selezioni.** Nel quadro delle attività delle pubbliche amministrazioni si procede comunque, di regola, alla pubblicazione di graduatorie e di esiti di concorsi e selezioni pubbliche.

Ad esempio, le graduatorie dei vincitori di concorsi per accedere agli impieghi nelle pubbliche amministrazioni o per attribuire specifici incarichi professionali devono essere pubblicate nel bollettino ufficiale della Presidenza del Consiglio dei ministri o dell'amministrazione interessata, dandone, se previsto, contestuale avviso sulla Gazzetta Ufficiale (27). Un analogo regime di conoscibilità è previsto per le procedure di reclutamento dei professori universitari di ruolo e dei ricercatori, con riferimento alle informazioni contenute nelle relazioni riassuntive dei lavori svolti dalle commissioni giudicatrici per le valutazioni comparative e negli annessi giudizi individuali e collegiali espressi sui candidati (28).

La diffusione, che l'amministrazione può lecitamente porre in essere in base a specifiche previsioni legislative o regolamentari, deve avere ad oggetto solo i dati personali pertinenti e non eccedenti ai fini del corretto espletamento della procedura concorsuale e della sua rispondenza ai parametri stabiliti nel bando (elenchi nominativi ai quali vengano abbinati i risultati di prove intermedie, elenchi degli ammessi alle prove scritte o orali, punteggi riferiti a singoli argomenti di esame; punteggi totali ottenuti).

Non risulta lecito riportare negli atti delle graduatorie da pubblicare altre tipologie di informazioni non pertinenti quali, ad esempio, recapiti di telefonia fissa o mobile o il codice fiscale [(29)].

Anche in tale ambito i soggetti pubblici possono avvalersi di nuove tecnologie per facilitare le comunicazioni con gli interessati riguardanti concorsi o selezioni pubbliche, mediante, ad esempio, la ricezione on-line di domande di partecipazione a concorsi e selezioni, corredate di diversi dati personali. A tale proposito va rilevato che le previsioni normative che disciplinano la pubblicazione di graduatorie, esiti e giudizi concorsuali rendono, in linea generale, lecita l'operazione di diffusione dei relativi dati personali a prescindere dal mezzo utilizzato.

La disciplina sulla protezione dei dati personali regola (v. art. 19, c. 3, del Codice) la diffusione di tali informazioni in maniera tendenzialmente uniforme, sia che essa avvenga attraverso una pubblicazione cartacea, sia attraverso la messa a disposizione su Internet mediante una pagina *web* [(30)].

Va tuttavia evidenziato che le caratteristiche di Internet consentono a chiunque, per effetto dei comuni motori di ricerca esterni ai siti, reperire indiscriminatamente e in tempo reale un insieme consistente di informazioni personali rese disponibili in rete, più o meno aggiornate e di natura differente [(31)].

Nell'utilizzare tale strumento di diffusione occorre, quindi, prevedere forme adeguate di selezione delle informazioni che potrebbero essere altrimenti aggregate massivamente mediante un comune motore di ricerca esterno ai siti. Si pensi alle pagine web contenenti dati relativi a esiti, graduatorie e giudizi di valutazione, che in termini generali dovrebbero essere conosciute più

appropriatamente solo consultando un determinato sito Internet, oppure attribuendo solo alle persone interessate una chiave personale di accesso (a vari dati relativi alla procedura, oppure solo a quelli che li riguardano), o predisponendo, nei siti istituzionali, aree ad accesso parimenti selezionato nelle quali possono essere riportate ulteriori informazioni accessibili anche ai controinteressati [(32)].

Ancorché, talvolta, la disciplina normativa di settore preveda espressamente forme specifiche e circoscritte di divulgazione (mediante, ad esempio, la sola messa a disposizione di documenti presso gli uffici o la sola affissione di atti in bacheche nei locali dell'amministrazione, ovvero mediante materiale affissione all'albo pretorio [(33)]),tali forme di pubblicazione non autorizzano, di per sé, a trasporre tutti i documenti contenenti dati personali così pubblicati in una sezione del sito Internet dell'amministrazione liberamente consultabile. Al tempo stesso, ciò non preclude all'amministrazione di riprodurre in rete alcuni dei predetti documenti, sulla base di una valutazione responsabile e attenta ai limiti posti dai princìpi di pertinenza e non eccedenza.

In ogni caso, è ovviamente consentita la diffusione in Internet di un avviso che indichi il periodo durante il quale determinati documenti sono consultabili presso l'amministrazione [(34)].

6.2 **Dati relativi all'organizzazione degli uffici, alla retribuzione e ai titolari di cariche e incarichi pubblici.** Alcuni specifici obblighi normativi -taluni dei quali si richiamano di seguito a titolo meramente esemplificativo- impongono ad amministrazioni pubbliche di rendere noti, attraverso i propri siti Internet, determinati dati personali concernenti i propri dipendenti (es. organigramma degli uffici con l'elenco dei nominativi dei dirigenti; elenco delle caselle di posta elettronica istituzionali attive). [(35)]

Tali dati, sebbene siano di fatto disponibili in Internet, sono utilizzabili da terzi (in particolare, gli indirizzi di posta elettronica) solo in relazione ad eventi, comunicazioni e scopi correlati alle funzioni istituzionali e al ruolo ricoperto dall'interessato all'interno dell'amministrazione. I medesimi dati non sono quindi utilizzabili liberamente da chiunque per inviare, ad esempio, comunicazioni elettroniche a contenuto commerciale o pubblicitario [(36)].

In virtù della disciplina sul riordino della dirigenza statale le amministrazioni dello Stato possono altresì diffondere in Internet i dati personali dei dirigenti inquadrati nei ruoli istituiti da ciascuna amministrazione (art. 23 d.lg. 30 marzo 2001, n. 165), nel rispetto dei princìpi di completezza, esattezza, aggiornamento, pertinenza e non eccedenza dei dati (art. 11 del Codice) (37).

Altre disposizioni di settore prevedono, inoltre, specifici regimi di pubblicità per talune informazioni personali concernenti le retribuzioni, i livelli stipendiali o le situazioni patrimoniali di titolari di cariche e incarichi pubblici.

A titolo meramente esemplificativo, si menziona il caso delle amministrazioni e degli organismi tenuti a pubblicare sui propri siti Internet i compensi e le retribuzioni degli amministratori delle società partecipate direttamente o indirettamente dallo Stato, dei dirigenti con determinato incarico (conferito ai sensi dell'art. 19, comma 6, del d.lg. 30 marzo 2001, n. 165), nonché dei consulenti, dei membri di commissioni e di collegi e dei titolari di qualsivoglia incarico corrisposto dallo Stato, da enti pubblici o da società a prevalente partecipazione pubblica non quotate in borsa (38).

Un ampio regime di conoscibilità è previsto da specifiche disposizioni legislative anche per i livelli stipendiali e le situazioni patrimoniali di parlamentari e consiglieri di enti locali, seppure mediante differenti modalità di diffusione (39). Alcune disposizioni permettono inoltre al datore di lavoro pubblico di acquisire, ma non di pubblicare, taluni dati personali relativi alla situazione patrimoniale dei propri dirigenti e, se vi consentono, del coniuge e dei figli conviventi, previa idonea informativa sul trattamento che ne verrà effettuato (art. 13 del Codice). Le medesime disposizioni non consentono, tuttavia, alle amministrazioni di conoscere l'integrale contenuto delle dichiarazioni dei redditi, nelle quali possono essere contenute informazioni eccedenti rispetto alla ricostruzione della situazione patrimoniale degli interessati, alcune delle quali aventi –peraltro- anche natura "sensibile" (si pensi, ad esempio, ad alcune particolari tipologie di spese per le quali sono riconosciute apposite detrazioni d'imposta) (40).

6.3. **Atti in materia di organizzazione degli uffici.** Salvo che ricorra una delle ipotesi sopra richiamate o previste da specifiche disposizioni legislative o regolamentari, non è di regola lecito diffondere informazioni personali riferite a singoli lavoratori attraverso la loro pubblicazione in comunicazioni e documenti interni affissi nei luoghi di lavoro o atti e circolari destinati alla collettività dei lavoratori, come nelle ipotesi di informazioni riguardanti contratti individuali di lavoro, trattamenti stipendiali o accessori percepiti, assenze dal lavoro per malattia, ferie, permessi, iscrizione e/o adesione di singoli dipendenti ad associazioni.

In presenza di disposizioni legislative o regolamentari che prevedono forme di pubblicazione obbligatoria delle deliberazioni adottate dall'amministrazione (41) o degli atti conclusivi di taluni procedimenti amministrativi occorre, poi, valutare con attenzione le stesse tecniche di redazione dei provvedimenti e delle deliberazioni in materia di organizzazione del personale. Nel rispetto dell'obbligo di adeguata motivazione degli atti amministrativi (42) vanno pertanto selezionate le informazioni da diffondere alla luce dei princìpi di pertinenza e indispensabilità rispetto alle finalità perseguite dai singoli provvedimenti, anche in relazione al divieto di diffusione dei dati idonei a rivelare lo stato di salute (artt. 11 e 22 del Codice). Un'attenta valutazione, nei termini sopra richiamati, è indispensabile soprattutto quando vengono in considerazione informazioni sensibili o di carattere giudiziario: si pensi, ad esempio, agli atti in materia di concessione dei benefici previsti dalla legge 5 febbraio 1992, n. 104 e ai provvedimenti di irrogazione di sanzioni disciplinari o relativi a controversie giudiziarie nelle quali siano coinvolti singoli dipendenti (43).

Con specifico riferimento alle finalità di applicazione della disciplina in materia di concessione di benefici economici o di abilitazioni, ad esempio, il trattamento può comprendere la diffusione dei dati sensibili nei soli casi in cui ciò sia indispensabile per la trasparenza delle attività medesime, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando, comunque, il divieto di diffusione dei dati idonei a rivelare lo stato di salute (art. 68, comma 3, del Codice).

Ove costituiscano presupposto dei provvedimenti adottati, tali informazioni vanno riportate solo negli atti a disposizione negli uffici consultabili esclusivamente da interessati e controinteressati, omettendo quindi di dettagliarle nel corpo degli atti da pubblicare e richiamandone soltanto gli estremi e/o un estratto dei relativi atti d'ufficio.

6.4. **Cartellini identificativi.** Analogamente, determina un'ipotesi di diffusione dei dati personali l'esibizione degli stessi su cartellini identificativi, appuntati, ad esempio, sull'abito o sulla divisa del personale di alcune strutture della pubblica amministrazione o di concessionari pubblici, in attuazione di taluni atti amministrativi di natura organizzativa, a livello sia nazionale, sia locale [(44)].

Nell'ambito del lavoro alle dipendenze delle pubbliche amministrazioni i cartellini identificativi possono rappresentare un valido strumento per garantire trasparenza ed efficacia dell'azione amministrativa [(45)], nonché per migliorare il rapporto fra operatori ed utenti.

Nel selezionare i dati personali destinati ad essere diffusi attraverso i cartellini identificativi, le amministrazioni sono tenute a rispettare i princìpi di pertinenza e non eccedenza dei dati in rapporto alle finalità perseguite (art. 11 del Codice), specie in assenza di necessarie disposizioni di legge o regolamento che prescrivano l'adozione per determinati dipendenti di cartellini identificativi e ne individuino eventualmente anche il relativo contenuto.

In tali ipotesi, alla luce di specifiche esigenze di personalizzazione e di umanizzazione del servizio e/o di collaborazione da parte dell'utente può risultare giustificato, in casi particolari e con riferimento a determinate categorie di dipendenti, riportare nei cartellini elementi identificativi ulteriori rispetto alla qualifica, al ruolo professionale, alla fotografia o ad un codice identificativo quali, ad esempio, le loro generalità (si pensi alle prestazioni sanitarie in regime di ricovero ospedaliero e al rapporto fiduciario che si instaura tra il paziente e gli operatori sanitari coinvolti).

7. Impronte digitali e accesso al luogo di lavoro

Anche nell'ambito del pubblico impiego [(46)], non è consentito utilizzare in modo generalizzato sistemi di rilevazione automatica delle presenze dei dipendenti mediante la raccolta di dati biometrici, specie se ricavati dalle impronte digitali. I dati biometrici, per la loro peculiare natura, richiedono l'adozione di elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta digitale, partendo dal modello di riferimento *(template)*, e la sua ulteriore "utilizzazione" a loro insaputa.

7.1. **Princìpi generali.** Il trattamento dei dati personali relativi alla rilevazione dell'orario di lavoro è riconducibile alle finalità perseguite dai soggetti pubblici quali datori di lavoro legittimati ad accertare il rispetto dell'orario di lavoro mediante *"forme di controlli obiettivi e di tipo automatizzato"* [(47)] (e in taluni casi a garantire speciali livelli di sicurezza), ma deve essere effettuato nel pieno rispetto della disciplina in materia di protezione dei dati personali.

Il principio di necessità impone a ciascuna amministrazione titolare del trattamento di accertare se la finalità perseguita possa essere realizzata senza dati biometrici o evitando ogni eccesso nel loro utilizzo che ne comporti un trattamento sproporzionato (artt. 3 e 11 del Codice). Devono essere quindi valutati preventivamente altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche che possano assicurare una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro.

Resta in particolare privo di giuridico fondamento l'utilizzo di sistemi di rilevazione delle impronte digitali per verificare l'esatto adempimento di prestazioni lavorative, ove siano attivabili misure "convenzionali" non lesive dei diritti della persona quali, ad esempio, apposizioni di firme anche in presenza di eventuale personale incaricato, fogli di presenza o sistemi di timbratura mediante *badge* magnetico.

Di regola, non è pertanto consentito il trattamento di dati relativi alle impronte digitali per accertare le ore di lavoro prestate effettivamente dal personale dislocato anche in sedi distaccate o addetto a servizi esterni, con riferimento, ad esempio, all'esigenza di computare con sistemi oggettivi le turnazioni, l'orario flessibile, il recupero, i permessi, il lavoro straordinario, i buoni pasto, nonché di prevenire eventuali usi abusivi o dimenticanze del *badge*.

Non può desumersi alcuna approvazione implicita dal semplice inoltro al Garante di note relative a progetti di installazione di impianti di rilevazione di impronte digitali, cui eventualmente non segua un esplicito riscontro dell'Autorità.

7.2. **Casi particolari.** Di regola, sistemi di rilevazione di impronte digitali nel luogo di lavoro possono essere quindi attivati soltanto per particolari esigenze di controllo dell'accesso a speciali aree dei luoghi di lavoro in cui si debbano assicurare elevati e specifici livelli di sicurezza, in relazione a specifiche necessità quali, ad esempio, la destinazione dell'area interessata:

1. allo svolgimento di attività aventi particolare carattere di segretezza, ovvero prestate da personale selezionato e impiegato in attività che comportano la necessità di trattare informazioni rigorosamente riservate (es. accesso a sale operative ove confluiscono segnalazioni afferenti alla sicurezza anticrimine; aree adibite ad attività inerenti alla difesa e alla sicurezza dello Stato; ambienti di torri di controllo aeroportuali);
2. alla conservazione di oggetti di particolare valore o la cui disponibilità deve essere ristretta ad un numero circoscritto di dipendenti in quanto un loro utilizzo improprio può determinare una grave e concreta situazione di rischio per la salute e l'incolumità degli stessi o di terzi (es. ambienti ove sono custodite sostanze stupefacenti o psicotrope).

Nelle ipotesi sopramenzionate il trattamento di dati relativi alle impronte digitali è ammesso a condizione che:

- sia sottoposto con esito positivo –di regole, a seguito di un interpello del titolare [(48)] - alla verifica preliminare, che

l'Autorità si riserva di effettuare ai sensi dell'art. 17 del Codice anche per determinate categorie di titolari o di trattamenti;

- venga effettuata preventivamente la notificazione al Garante (artt. 37, comma 1, lett. a) e 38 del Codice);
- non sia comunque registrata l'immagine integrale dell'impronta digitale, bensì solo il modello di riferimento da essa ricavato *(template)*;
- tale modello non sia archiviato in una memoria centralizzata, bensì in un supporto posto nell'esclusiva disponibilità dell'interessato (*smart card* o dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale);
- sia fornita ai dipendenti interessati un'informativa specifica per il trattamento in questione (art. 13 del Codice).

8. Dati idonei a rivelare lo stato di salute

8.1. **Dati sanitari. Il datore di lavoro pubblico deve osservare** cautele particolari anche per il trattamento dei dati sensibili (artt. 4, comma 1, lett. d), 20 e 112 del Codice) e, segnatamente, di quelli idonei a rivelare lo stato di salute.

Nel trattamento di queste informazioni l'amministrazione deve rispettare anzitutto i princìpi di necessità e di indispensabilità, valutando specificamente il rapporto tra i dati sensibili e gli adempimenti derivanti da compiti e obblighi di volta in volta previsti dalla legge (artt. 20 e 22 del Codice). È importante valorizzare tali princìpi nell'applicare disposizioni di servizio e regolamenti interni precedenti alla disciplina in materia di protezione dei dati personali.

In tale quadro non risultano, ad esempio, lecite le modalità - utilizzate da amministrazioni militari e forze di polizia, a fini di organizzazione del lavoro e/o di turni di servizio- che prevedono la redazione di un elenco nominativo di ufficiali o agenti in licenza, recante:

- l'indicazione "per convalescenza" o "in aspettativa", per regolare l'accesso alla caserma del personale assente dal servizio (49);
- l'indicazione, su ordini di servizio o altri atti affissi nei luoghi di lavoro, i motivi giustificativi delle assenze del personale (utilizzando, ad esempio, diciture quali "a riposo medico").

Particolari accorgimenti per la gestione dei dati sensibili possono essere previsti anche da norme estranee al Codice in materia di protezione dei dati personali, ma volte comunque a contenere, nei limiti dell'indispensabile, i dati dei quali il datore di lavoro può venire a conoscenza per instaurare e gestire il rapporto di lavoro (50). La disciplina contenuta nel Codice deve essere quindi coordinata e integrata (cfr. punto 3.2.) con altre regole settoriali (51) o speciali (52).

8.2. **Assenze per ragioni di salute.** Riguardo al trattamento di dati idonei a rivelare lo stato di salute, la normativa sul rapporto di lavoro e le disposizioni contenute in contratti collettivi possono giustificare il trattamento dei dati relativi a casi di infermità che

determinano un'incapacità lavorativa (temporanea o definitiva), con conseguente accertamento di condizioni di salute del lavoratore da parte dell'amministrazione di appartenenza (53), anche al fine di accertare l'idoneità al servizio, alle mansioni o allo svolgimento di un proficuo lavoro (54).

Tra questi ultimi può rientrare anche una informazione relativa all'assenza dal servizio per malattia, indipendentemente dalla circostanza che sia contestualmente indicata esplicitamente la diagnosi (55).

Non diversamente, il datore di lavoro può in vari casi trattare legittimamente dati sensibili relativi all'invalidità o all'appartenenza a categorie protette, nei modi e per le finalità prescritte dalla vigente normativa in materia (art. 112, comma 2, lett. a) del Codice) (56).

A tale riguardo va rilevata la sussistenza di specifici obblighi normativi nei riguardi del lavoratore per consentire al datore di lavoro di verificare le sue reali condizioni di salute nelle forme di

legge [(57)]. Per attuare tali obblighi è ad esempio previsto che venga fornita all'amministrazione di appartenenza un'apposita documentazione a giustificazione dell'assenza, consistente in un certificato medico contenente la sola indicazione dell'inizio e della durata presunta dell'infermità: c.d. *"prognosi"* [(58)]. In assenza di speciali disposizioni di natura normativa, che dispongano diversamente per specifiche figure professionali [(59)], il datore di lavoro pubblico non è legittimato a raccogliere certificazioni mediche contenenti anche l'indicazione della diagnosi [(60)].

Anche nei casi in cui la raccolta dei dati relativi alla diagnosi sia effettuata lecitamente sulla base di tali disposizioni, in conformità ai princìpi di proporzionalità e indispensabilità, non è consentito all'amministrazione di appartenenza trascrivere nei documenti caratteristici o matricolari del personale le indicazioni sulla prognosi e la diagnosi contenute nei certificati prodotti dall'interessato per giustificare le assenze dal servizio (artt. 11, comma 1, lett. e) e 22, comma 9, del Codice) [(61)]. A tale riguardo, va anzi rilevato che, qualora il lavoratore produca documentazione medica recante anche l'indicazione della diagnosi insieme a quella della prognosi, l'amministrazione (salvi gli speciali casi eventualmente previsti nei termini sopra indicati) deve astenersi dall'utilizzare ulteriormente tali informazioni (art. 11, comma 2, del Codice) invitando anche il personale a non produrne altri con le medesime caratteristiche [(62)].

In linea generale, all'esito delle visite di controllo sullo stato di infermità -effettuate da medici dei servizi sanitari pubblici (art. 5 l. 20 maggio 1970, n. 300) [(63)] -, il datore di lavoro pubblico è legittimato a conoscere i dati personali dei lavoratori riguardanti la capacità o l'incapacità al lavoro e la prognosi riscontrata, con esclusione di qualsiasi informazione attinente alla diagnosi [(64)].

In tale quadro, il datore di lavoro può, al fine di far valere i propri diritti in relazione a fenomeni di ritenuto assenteismo e di eventuale non veritiera certificazione sanitaria, redigere note informative, segnalazioni o denunce contenenti anche riferimenti circostanziati alle ragioni e alle modalità delle singole assenze e individuandone i destinatari nel rispetto dei princìpi di indispensabilità, pertinenza e non eccedenza [(65)].

Sulla base degli elementi acquisiti da segnalazioni e quesiti pervenuti all'Autorità, risulta giustificata, alla luce delle disposizioni

contenute nei contratti collettivi, la conoscenza da parte dell'amministrazione di appartenenza di informazioni personali relative all'effettuazione di visite mediche, prestazioni specialistiche o accertamenti clinici, nonché alla presenza di patologie che richiedono terapie invalidanti (66), quando il dipendente richiede di usufruire del trattamento di malattia o di permessi retribuiti per le assenze correlate a tali esigenze.

8.3. **Denuncia all'Inail.** Per dare esecuzione ad obblighi di comunicazione relativi a dati sanitari, in taluni casi il datore di lavoro può anche venire a conoscenza delle condizioni di salute del lavoratore.

Tra le fattispecie più ricorrenti deve essere annoverata la denuncia all'istituto assicuratore (Inail) avente ad oggetto infortuni e malattie professionali occorsi ai lavoratori; essa, infatti, per espressa previsione normativa, deve essere corredata da specifica certificazione medica (artt. 13 e 53 d.P.R. n. 1124/1965).

In tali casi l'amministrazione, pur potendo conoscere la diagnosi, deve comunicare all'ente assicurativo solo le informazioni sanitarie relative o collegate alla patologia denunciata, anziché dati sulla salute relativi ad altre assenze che si siano verificate nel corso del rapporto di lavoro, la cui eventuale comunicazione sia eccedente e non pertinente –con la conseguente loro inutilizzabilità–, trattandosi di dati non rilevanti nel caso oggetto di denuncia (art. 11, commi 1 e 2, del Codice) (67).

8.4. **Visite medico-legali.** Le pubbliche amministrazioni possono trattare legittimamente dati idonei a rivelare lo stato di salute dei propri dipendenti, non solo per accertare, anche d'ufficio, attraverso le strutture sanitarie pubbliche competenti, la persistente idoneità al servizio, alle mansioni o allo svolgimento di un proficuo lavoro (68), ma anche per riconoscere la dipendenza da causa di servizio, per concedere trattamenti pensionistici di privilegio o l'equo indennizzo (69) ovvero per accertare, sempre per fini pensionistici, la sussistenza di stati invalidanti al servizio o di inabilità non dipendenti da causa di servizio (artt. 20 e 112, comma 2, lett. d) del Codice) (70).

Nel disporre tali accertamenti le amministrazioni possono comunicare ai collegi medici competenti i dati personali sensibili del dipendente dei quali dispongano, nel rispetto del principio di indispensabilità (art. 22, commi 1, 5 e 9) (71); devono inoltre conformare il trattamento dei dati sanitari del lavoratore secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato, anche in riferimento al diritto alla protezione dei dati personali (cfr. par. 4.3) (72).

Analoghi accorgimenti devono essere adottati dagli organismi di accertamento sanitario all'atto sia della convocazione dell'interessato a visita medico-collegiale, sia della comunicazione dell'esito degli accertamenti effettuati all'amministrazione di appartenenza del lavoratore, ed eventualmente all'interessato medesimo. In particolare, nel caso di accertamenti sanitari finalizzati ad accertare l'idoneità al servizio, alle mansioni o a proficuo lavoro del dipendente, alla luce del principio di indispensabilità, i collegi medici devono trasmettere all'amministrazione di appartenenza dell'interessato il relativo verbale di visita con la sola indicazione del giudizio medico-legale di idoneità, inidoneità o di altre forme di inabilità (73).

Qualora siano trasmessi dagli organismi di accertamento sanitario verbali recanti l'indicazione della diagnosi dell'infermità o della lesione che determinano un'incapacità lavorativa, i datori di lavoro non possono, comunque, utilizzare ulteriormente tali informazioni (art. 11, comma 2, del Codice).

8.5. **Abilitazioni al porto d'armi e alla guida.** In conformità alle norme sulle autorizzazioni di polizia per la detenzione ed il porto d'armi, le amministrazioni possono di regola trattare i dati relativi agli esiti delle visite medico-legali cui sottopongono i propri dipendenti per consentire l'adozione da parte degli uffici competenti dei provvedimenti sull'arma di servizio, ove si tratti di agenti di pubblica sicurezza, abilitati al porto di pistola (74).

La normativa di settore e le disposizioni contenute nei contratti collettivi non autorizzano, invece, le pubbliche amministrazioni a comunicare agli uffici competenti del Dipartimento per i trasporti terrestri informazioni idonee a rivelare lo stato di salute dei propri

dipendenti, ancorché acquisite legittimamente, per consentire di verificare la persistenza in capo a questi ultimi dei requisiti fisici e psichici previsti dalla legge per il conseguimento della patente di guida [(75)]. Allo stato dell'attuale normativa tale attività comporta, infatti, un flusso di dati personali sensibili verso l'amministrazione dei trasporti che non risulta trovare una base di legittimazione in un'idonea disposizione normativa [(76)], né risulta altrimenti riconducibile alle finalità di rilevante interesse pubblico connesse alla gestione di rapporti di lavoro da parte dell'amministrazione di appartenenza dell'interessato (art. 112 del Codice) [(77)].

Siffatte operazioni di comunicazione non possono ritenersi lecite anche se effettuate da forze armate e di polizia che, in base al Codice della strada, provvedano direttamente nei riguardi del personale in servizio all'individuazione e all'accertamento dei requisiti necessari alla guida dei veicoli in loro dotazione e al rilascio del relativo titolo abilitativo [(78)], attesa la diversità dei presupposti per il conferimento (o l'eventuale sospensione o ritiro) della patente militare rispetto a quella civile e la sfera di discrezionalità ad esse conferite [(79)].

8.6. **Altre informazioni relative alla salute.** Devono essere presi in considerazione altri casi nei quali può effettuarsi un trattamento di dati relativi alla salute del lavoratore (e anche di suoi congiunti), al fine di permettergli di godere dei benefici di legge: si pensi, ad esempio, alle agevolazioni previste per l'assistenza a familiari disabili, ai permessi retribuiti e ai congedi per gravi motivi familiari.

In attuazione dei princìpi di indispensabilità, pertinenza e non eccedenza, in occasione di istanze volte ad usufruire dei congedi a favore dei lavoratori con familiari disabili in situazione di gravità, l'amministrazione di appartenenza non deve venire a conoscenza di dati personali del congiunto portatore di handicap relativi alla diagnosi o all'anamnesi accertate dalle commissioni mediche indicate dall'art. 4 della l. 5 febbraio 1992, n. 104 [(80)]. A tal fine, infatti, il lavoratore deve presentare al datore di lavoro una certificazione dalla quale risulti esclusivamente l'accertata condizione di handicap grave per opera delle commissioni mediche di cui all'art. 1 della legge 15 ottobre 1990, n. 295 [(81)].

Diversamente, per usufruire di permessi o congedi per gravi infermità o altri gravi motivi familiari, il lavoratore è tenuto per legge a produrre alla propria amministrazione idonea documentazione medica attestante le gravi infermità o le gravi patologie da cui risultano affetti i propri familiari [(82)].

Allo stesso modo, il datore di lavoro può venire a conoscenza dello stato di tossicodipendenza di un proprio dipendente o di un familiare di questi, in caso di richieste di accesso o concorso a programmi riabilitativi o terapeutici con conservazione del posto di lavoro (senza retribuzione), atteso l'onere di presentare (nei termini prescritti dai contratti collettivi e dagli accordi di lavoro per il pubblico impiego) specifica documentazione medica al datore di lavoro (83).

9. Dati idonei a rivelare le convinzioni religiose

Analoghe cautele devono essere osservate nel trattamento di altre tipologie di informazioni sensibili relative al lavoratore, quali quelle idonee a rivelarne le convinzioni religiose. Il trattamento di queste informazioni deve ritenersi in via generale lecito soltanto ove risulti indispensabile per la gestione da parte dei soggetti pubblici del rapporto di lavoro e di impiego, e, in particolare, per consentire l'esercizio delle libertà religiose riconosciute ai lavoratori appartenenti a determinate confessioni, in conformità alle disposizioni di legge e di regolamento che regolano i rapporti tra lo Stato e le medesime confessioni.

Ad esempio, i dati sulle convinzioni religiose possono venire in considerazione per la concessione dei permessi per festività religiose su specifica richiesta dell'interessato motivata per ragioni di appartenenza a una determinata confessione [(84)]. Le convinzioni religiose potrebbero emergere, inoltre, in relazione al contesto in cui sono trattate o al tipo di trattamento effettuato, da alcune particolari scelte del lavoratore, rispondenti a determinati dettami religiosi, per il servizio di mensa eventualmente apprestato presso il luogo di lavoro.

Inoltre, in base alle specifiche norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi, le prove del concorso scritte e orali non possono aver luogo, ai sensi della legge 8 marzo 1989, n. 101 , nei giorni di festività religiose ebraiche rese note con decreto del Ministro dell'interno mediante pubblicazione nella Gazzetta Ufficiale della Repubblica, nonché nei giorni di festività religiose valdesi [(85)].

In tale quadro, pertanto, nel fissare il diario delle prove concorsuali per l'accesso ai pubblici impieghi, non risulta giustificata la raccolta sistematica e preventiva dei dati relativi alle convinzioni religiose dei predetti candidati [(86)] essendo sufficiente fissare le prove in giorni non coincidenti con dette festività.

---

(1) Provv. 23 novembre 2006, n. 53, in *www.garanteprivacy.it*, doc. web n. 1364099, e in G.U. 7 dicembre 2006, n. 285.
(2) Anche per le presenti linee guida si è tenuto conto della Raccomandazione n. R (89) 2 del Consiglio d'Europa relativa alla protezione dei dati a carattere personale utilizzati ai fini dell'occupazione, del Parere n. 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione, reso il 13 settembre 2001 dal Gruppo Art. 29 dei Garanti europei (in *http://ec.europa.eu*), nonché del Code of practice, *"Protection of workers' personal data"*, approvato dall'Organizzazione internazionale del lavoro (Oil).
(3) Art. 2, comma 2, del Codice.
(4) Art. 2, comma 5, del Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82 così come modificato dal d.lg. 4 aprile 2006, n. 159).
(5) L'organizzazione sindacale potrà a sua volta comunicare a terzi o diffondere i dati personali ottenuti dall'amministrazione soltanto previa acquisizione del consenso informato dei dipendenti interessati o di altro presupposto equipollente (art. 24 del Codice).
(6) Provv. 30 dicembre 2003, in www.garanteprivacy.it, doc. web n. 1085621.
(7) Note 9 dicembre 1997, ivi, doc. web nn. 30915 e 39785.
(8) Cfr. circolare Ispesl 3 marzo 2003, n. 2260.
(9) Art. 4, comma 8, d.lg. 19 settembre 1994, n. 626.
(10) Provv. 23 novembre 2006, in *www.garanteprivacy.it*, doc. web n. 1364099.
(11) Provv. 9 novembre 2005, in *www.garanteprivacy.it*, doc. web n. 1191411.
(12) A titolo di esempio, oltre ad alcuni regolamenti concernenti amministrazioni centrali (Ministero della difesa, d.m. 13 aprile 2006, n. 203, in G.U. 1° giugno 2006, n. 126; Ministero dell'interno, d.m. 21 giugno 2006, n. 244, in G.U. 9 agosto 2006, n. 184, S.O.; Ministero della pubblica istruzione, d.m. 7 dicembre 2006, n. 305, in G.U. 15 gennaio 2007, n. 11; Ministero delle

infrastrutture, d.m. 9 febbraio 2007, n. 21, in G.U. 16 marzo 2007, n. 63; Ministero della giustizia, d.m. 12 dicembre 2006, n. 306, in G.U. 15 gennaio 2007, n. 11; Ministero dell'università e della ricerca, d.m. 28 febbraio 2007, n. 54, in G.U. 26 aprile 2007, n. 96), si segnalano taluni schemi tipo di regolamento relativi ad enti locali (in *www.garanteprivacy.it*, doc. web n. 1174532), comunità montane (doc. web n. 1182195) e province (doc. web n. 1175684).
(13) Provv. 30 giugno 2005, in *www.garanteprivacy.it*, doc. web n. 1144445.
(14) Art. 50 d.lg. 30 marzo 2001, n. 165 con riferimento alla trasmissione alla Presidenza del Consiglio dei ministri di informazioni nominative relative al personale che ha fruito di distacchi, permessi cumulativi sotto forma di distacco, aspettative e permessi per attività sindacale o per funzioni pubbliche elettive, al fine del contenimento, della trasparenza e della razionalizzazione delle aspettative e dei permessi sindacali nel settore pubblico.
(15) Artt. 59 e 60 del Codice. Si vedano anche gli artt. 22 e ss. l. 7 agosto 1990, n. 241; d.P.R. 12 aprile 2006, n. 184; art. 8 d.P.R. 27 giugno 1992, n. 352;artt. 10 e 43 d.lg. 18 agosto 2000, n. 267.
(16) Cfr. par. 5.1 e 5.2 delle presenti linee guida.
(17) Relazione annuale per il 2004 del Garante, p. 81.
(18) Provv. 12 maggio 2005, in *www.garanteprivacy.it*, doc. web 1137798.
(19) Cfr. art. 6 Ccnl relativo al personale del comparto scuola del 24 luglio 2003.
(20) Cfr. art. 40, comma 4, d.lg. n. 165/2001 e art. 28 l. 20 maggio 1970, n. 300. Si vedano anche Corte cass. 17 aprile 2004, n. 7347; Corte d'appello Torino 16 luglio 2003 in Rivista giuridica del lavoro e della previdenza sociale, 2002, parte I, p. 116; par. 7 Raccomandazione del Consiglio d'Europa n. R (89)2; par. 10.10. del Code of practice dell'Oil.
(21) Si veda, ad es., art. 37 Ccnl del personale del comparto "ministeri" del 16 maggio 1995; art. 48 del Ccnl del personale del comparto "sanità" del 1° settembre 1995; art. 6 del Ccnl del personale del comparto "università" del 9 agosto 2000; art. 6, Ccnl del personale del comparto enti art. 70 d.lg. 165/2001 del 14 febbraio 2001; art. 37 Ccnl del personale del comparto delle "Istituzioni e degli enti di ricerca e sperimentazione" del 21 febbraio 2002; art. 7 Ccnl del personale del comparto delle regioni-autonomie locali del 6 luglio 1995; art. 7 Ccnl del personale del comparto regioni ed autonomie locali personale non dirigente del 1°aprile 1999.
(22) Si veda, ad es., Consiglio di Stato sez. IV, 5 maggio 1998, n. 752; Tar Lombardia Milano, sez.I, 31 luglio 2002, n. 3261;; Tar Emilia-Romagna 10 gennaio 2003, n. 16; Tar Calabria, sez. II, 11 luglio 2005, n. 1165; Commissione per l'accesso ai documenti amministrativi, pareri 6 luglio 2004, n. 8 e 28 giugno 2006, n. 51.
(23) Si vedano ad es. cfr. art. 12 Ccnl del personale dirigente dell'area 1 del 5 aprile 2001; art. 11, Ccnl segretari comunali e provinciali del 16 maggio 2001; art. 13 Ccnl relativo al quadriennio normativo 1998-2001 del personale del comparto università.
(24) Artt. 111 e 104 d.P.R. 10 gennaio 1957, n. 3.
(25) Cfr. Provv. 27 febbraio 2002 (doc. web n. 1063639), con il quale il Garante ha vietato la diffusione di dati idonei a rivelare lo stato di salute

riportati in una graduatoria dei trasferimenti affissa nella bacheca di un provveditorato agli studi.
(26) Cfr. Relazione annuale del Garante 2004, p. 83.
(27) Art. 15 d.P.R. 9 maggio 1994, n. 487; v. anche art. 4 d.P.R. 21 settembre 2001, n. 446; art. 18, comma 6, d.P.R. 27 marzo 2001, n. 220; art. 8 d.P.R. 28 luglio 2000, n. 271; art. 2 d.P.R. 28 luglio 2000, n. 272; art. 2 d.P.R. 28 luglio 2000, n. 270; art. 52, comma 2, r.d. 12 ottobre 1933, n. 1364.
(28) Cfr. art. 6 d.P.R. 23 marzo 2000, n. 117.
(29) Provv. 19 aprile 2007 recante "Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali".
(30) Cfr. Comunicato stampa del Garante del 14 giugno 1999.
(31) Cfr. Provv.10 novembre 2004, doc. web n. 1116068; cfr. anche Newsletter 21-27 marzo 2005.
(32) Cfr. Provv. 19 aprile 2007, cit.
(33) Cfr., ad es., art. 6, comma 6, d.P.R. n. 487/1994 con riferimento agli esiti delle prove intermedie dei concorsi per accedere agli impieghi nelle pubbliche amministrazioni e art. 25, comma 3, r.d. 22 gennaio 1934, n. 37, con riferimento all'elenco degli ammessi alla prove orali per l'abilitazione alla professione di avvocato.
(34) Cfr. Provv. 19 aprile 2007, cit.
(35) Art. 54 d.lg. 7 marzo 2005, n. 82.
(36) Cfr. Provv. 19 dicembre 2002, doc. web n. 1067231.
(37) Cfr. art. 23 d.lg. n. 165/ 2001 e artt. 1, comma 7 e 2, comma 4, d.P.R. 23 aprile 2004, n. 108.
(38) Art. 1, comma 593, l. 27 dicembre 2006, n. 296.
(39) Cfr. l. 5 luglio 1982, n. 441. Si veda anche Newsletter del Garante 4-10 giugno 2001 e Corte di giustizia delle Comunità europee, 20 maggio 2003, causa C-465/2000.
(40) Cfr. art. 17, comma 22, l. 15 maggio 1997, n. 127. Si veda anche Parere 8 giugno 1999, doc. web n. 40369. Analoga disciplina vige anche per magistrati, avvocati dello Stato e procuratori, professori e ricercatori universitari di livello dirigenziale od equiparato.
(41) Cfr. art. 10 e 124 d.lg. n. 267/2000.
(42) Art. 3, comma 3, l. n. 241/1990.
(43) Cfr. Provv. 27 febbraio 2002, doc. web 1063639, Provv. 9 dicembre 2003 e Provv. 17 aprile 2003, doc. web n. 1054640. Si vedano anche, con particolare riferimento alle deliberazioni degli enti locali, Provv. 19 aprile 2007 cit. e Provv. 25 gennaio 2007, doc. web 1386836.
(44) Cfr. parte seconda, 2.3.1, b.3), d.P.C.M. 21 dicembre 1992; art. 1.1. e all. n. 8 art. 61 d.P.C.M. 19 maggio 1995; parte seconda, 2.5.1, d.P.C.M. 30 dicembre 1998 art. 4.2.2, provv. Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano 5 agosto 1999.
(45) Art.1, l. n. 241/1990.
(46) Per i dipendenti del settore privato v. Provv. 23 novembre 2006, doc. web n. 1364939.
(47) Cfr. art. 18 del Codice; art. 4 dell'accordo riguardante le tipologie degli orari di lavoro ai sensi dell'art. 19, comma 5, del Ccnl comparto ministeri del

16 maggio 1995, confermato dall'art. 26 del Ccnl del 12 giugno 2003. Si veda anche l'art. 17 Ccnl del comparto del personale delle regioni-autonomie locali del 6 luglio 1995, confermato dall'art. 45 del Ccnl del 22 gennaio 2004.
(48) Nell'interpello al Garante vanno specificate le caratteristiche tecnologiche delle apparecchiature utilizzate e le ragioni in base alle quali non si ritengono idonei, rispetto alle finalità da perseguire, altri sistemi o procedure che pongono minori pericoli o rischi per i diritti e le libertà fondamentali degli interessati.
(49) Cfr. Provv. 7 luglio 2004, doc. web n. 1068839.
(50) Cfr. artt. 8 e 38 l. n. 300/1970 e artt. 113 e 171 del Codice.
(51) Tra le quali, ad esempio, la richiamata disciplina contenuta nel d.lg. n. 626/1994 o nell'art. 5 della l. n. 300/1970 sugli accertamenti sanitari facoltativi.
(52) Si pensi ai divieti contenuti negli artt. 5 e 6 l. 5 giugno 1990, n. 135, in materia di Aids.
(53) Cfr. art. 5 l. n. 300/1970; si vedano anche le pertinenti disposizioni dei contratti collettivi relativi ai differenti comparti (art. 21, comma 10, Ccnl Comparto ministeri del 16 maggio 1995; art. 17, comma 12, Ccnl relativo al personale del comparto scuola del 24 luglio 2003, già art. 49, lettera g) del Ccnl del 26 maggio 1999 e art. 23, comma 12, del Ccnl del 4 agosto 1995; art. 34, comma 10, Ccnl del personale non dirigente del comparto università, del 9 agosto 2000; art. 17, comma 11, Ccnl relativo al personale del comparto delle istituzioni e degli enti di ricerca e sperimentazione del 21 febbraio 2002; art. 11, comma 12, Ccnl relativo al personale del comparto delle istituzioni di alta formazione e specializzazione artistica e musicale del 16 febbraio 2005).
(54) Cfr. art. 5, comma 3, l. n. 300/1970, art. 15, d.P.R. n. 461/2001, art. 21, comma 3, Ccnl Comparto ministeri del 16 maggio 1995; art. 17, comma 3, Ccnl relativo al personale del comparto scuola del 24 luglio 2003, già art. 23, comma 3, del Ccnl del 4 agosto 1995; art. 34, comma 3, Ccnl del personale non dirigente del comparto università, del 9 agosto 2000; art. 17, comma 4, Ccnl relativo al personale del comparto delle istituzioni e degli enti di ricerca e sperimentazione del 21 febbraio 2002; art. 11, comma 3, Ccnl relativo al personale del comparto delle istituzioni di alta formazione e specializzazione artistica e musicale del 16 febbraio 2005. Dall'accertamento in questione può, inoltre, conseguire l'attribuzione all'interessato di altri incarichi o mansioni, oppure la risoluzione del rapporto di lavoro e la conseguente adozione degli atti necessari per riconoscere trattamenti pensionistici alle condizioni previste dalle disposizioni di settore. Cfr. art. 8 d.P.R. 27 febbraio 1991 n. 132 (Corpo forestale dello Stato); art. 129 d.lg. 30 ottobre 1992, n. 443 (Corpo di polizia penitenziaria); art. 15 d.P.R. 29 ottobre 2001, n. 461; art. 99 l. 22 dicembre 1975, n. 685; tossicodipendenza; art 5 d.P.R. 20 febbraio 2001, n. 114 (carriera diplomatica); art. 5 d.P.R. 23 maggio 2001, n. 316 (carriera prefettizia); art. 2 d.m. 30 giugno 2003, n. 198 (Polizia di Stato).
(55) Cfr. Provv. 7 luglio 2004, doc. web n. 1068839. V. pure il punto 50 della sentenza della Corte di giustizia delle Comunità europee 6 novembre 2003 C-101/01, Lindqvist.
(56) Cfr. l. n. 68/1999 citata e l. 29 marzo 1985, n. 113.
(57) Provv. 15 aprile 2004, doc. web n. 1092564; Cfr. art. 5 l. n. 300/1970; si

vedano anche le pertinenti disposizioni dei contratti collettivi di lavoro applicabili ai diversi comparti come, ad esempio, l'art. 21 Ccnl comparto ministeri personale non dirigente del 16 maggio 1995.
(58) Cfr. art. 2 d.l. 30 dicembre 1979, n. 663, conv. in l., con mod., con l'art. 1 l. 29 febbraio 1980, n. 33, successivamente modificato dal comma 149 dell'art. 1 l. 30 dicembre 2004, n. 311.
(59) Cfr. art. 61 d.P.R. 28 ottobre 1985, n. 782 per il personale della Polizia di Stato.
(60) In tal senso si veda art. 17, comma 11, Ccnl relativo al personale del comparto scuola del 24 luglio 2003, già art. 49, lettera f) del Ccnl del 26 maggio 1999 e art. 23, comma 10, del Ccnl del 4 agosto 1995; art. 34,comma 9, Ccnl del personale non dirigente del comparto Università, del 9 agosto 2000; art. 17, comma 10, Ccnl relativo al personale del comparto delle istituzioni e degli enti di ricerca e sperimentazione del 21 febbraio 2002; art. 11, comma 11, Ccnl relativo al personale del comparto delle istituzioni di alta formazione e specializzazione artistica e musicale del 16 febbraio 2005.
(61) Cfr. art. 55 d.P.R. d.P.R. 10 gennaio 1957, n. 3 e art. 24 d.P.R. 3 maggio 1957 n. 686. Si veda anche Provv. 19 ottobre 2005, doc. web n. 1185148 con riferimento al servizio matricolare del Corpo della Guardia di finanza.
(62) Cfr. par. 1.1 delle presenti linee guida.
(63) Cfr. art. 2 d.l. 30 dicembre 1979, n. 663, conv. in l., con mod., con l'art. 1, l. 29 febbraio 1980, n. 33 e mod. dal comma 149 dell'art. 1 l. 30 dicembre 2004, n. 311. Si veda anche art. 14, lett. q), l. 23 dicembre 1978, n. 833.
(64) Art. 5 d.l. 12 settembre 1983, n. 463 conv., con mod., in l. 11 novembre 1983, n. 638 e art. 6, comma 3, d.m. 15 luglio 1986.
(65) Cfr. Provv. 24 settembre 2001, doc. web n. 39460 e 28 settembre 2001, doc. web n. 41103.
(66) Cfr. art. 17 Ccnl del personale del comparto scuola stipulato il 24 luglio 2003; art. 17 Ccnl del personale del comparto delle istituzioni e degli enti di ricerca e sperimentazione stipulato il 21 febbraio 2002; art. 34 Ccnl del personale non dirigente del comparto Università stipulato il 9 agosto 2000; art. 23 Ccnl del personale del comparto sanità stipulato il 1° settembre 1995 e art. 11 Ccnl integrativo stipulato il 20 settembre 2001; art. 21 Ccnl del personale del comparto ministeri stipulato il 16 maggio 1995 e art. 6 Ccnl integrativo stipulato il 16 maggio 2001. Si vedano anche i chiarimenti forniti dall'Aran in data 20 gennaio 2003 in relazione ai quesiti B14 e B16, in *www.aranagenzia.it*.
(67) In tal senso v. il Provv. 15 aprile 2004, doc. web n. 1092564.
(68) Art. 5, comma 3, l. n. 300/1970; art. 15 d.P.R. 29 ottobre 2001, n. 461.
(69) Cfr. d.P.R. 29 dicembre 1973, n.1092 e d.P.R. 29 ottobre 2001, n. 461.
(70) Cfr. art. 2, comma 12, l. 8 agosto 1995, n. 335; art. 13, l. 8 agosto 1991, n. 274; d.P.R. 29 ottobre 2001, n. 461.
(71) Artt. 7, 9, comma 2 e 15, comma 1, d.P.R. n. 461/2001.
(72) Cfr. Provv. 23 luglio 2004, doc. web n. 1099216.
(73) Art. 4, commi 3 e 4, d.P.R. n. 461/2001.
(74) Cfr. Provv. 22 gennaio 2004, doc. web n. 1086280; v. anche, per altri profili, Provv. 15 gennaio 2004, doc. web n. 1054663 e Trib. Venezia 14 luglio 2004, n. 340.
(75) Cfr. artt. 119 e 128–130 d.lg. 30 aprile 1992, n. 285.

(76) Cfr. d.lg. 30 aprile 1992, n. 285 e d.P.R. 16 dicembre 1992, n. 495.
(77) Cfr. artt. 119 e 128–130 d.lg. 30 aprile 1992, n. 285. In merito, poi, alle comunicazioni di dati personali sensibili da parte delle aziende sanitarie alle commissioni mediche locali per le patenti di guida si guardi il Provv. del Garante del 28 giugno 2006, doc. web n. 1322833.
(78) Art. 138 d.lg. n. 285/1992.
(79) Cfr. art. 138, commi 4 e 12, d.lg. n. 285/1992. Si veda anche Cons. Stato sez. IV, 14 maggio 2001, n. 2648.
(80) Cfr. Provv. 21 marzo 2007, doc. web n. 1395821.
(81) Cfr. art. 33 l. 5 febbraio 1992, n. 104; art. 4, comma 2, l. 8 marzo 2000, n. 53 e artt. 33 e 42 d.lg. 26 marzo 2001, n. 151; si veda anche Cass. civ., 17 agosto 1998, n. 8068.
(82) Art. 4, l. 8 marzo 2000, n. 53 e d.m. 21 luglio 2000, n. 278.
(83) Art. 124, commi 1 e 2, d.P.R. n. 309/1990.
(84) Art. 4, comma 2, l. 8 marzo 1989, n. 101 recante *"Norme per la regolazione dei rapporti tra lo Stato e l'Unione delle Comunità ebraiche italiane"*; art. 17, comma 2, l. 22 novembre 1988, n. 516 recante *"Norme per la regolazione dei rapporti tra lo Stato e l'Unione italiana delle Chiese cristiane avventiste del 7° giorno"*.
(85) Art. 6, comma 2, d.P.R. 9 maggio 1994, n. 487 *"Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi"*.
(86) Cfr. artt. 4, comma 2 e 5, l. n. 101/1989 e art. 17, comma 2, l. n. 516/1988 cit.

REGOLAMENTO PRIVACY

Il 07/12/2006 è stato emanato il D.M. n. 305 "**regolamento recante identificazione dei dati sensibili e giudizari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione**...". Questo è il regolamento che attendevamo da mesi, anzi, più o meno da un anno. Il testo si compone di pochi articoli e di sette schede che ne costituiscono parte integrante e sostanziale. Di fatto questo regolamento è immodificabile proprio perché non è una proposta, un fac-simile che il Ministero ha redatto, bensì una norma precisa che ha la sua collocazione precia nell'ordinamento delle fonti. Attenzione ad un'altra cosa: il regolamento NON DEVE ESSERE ADOTTATO dalla singole II.SS. perché l'adozione presuppone una facoltà di scelta che in questo caso non c'è. Occorre invece informare rapidamente ed adeguatamente tutti gli operatori sulle indicazioni e le prescrizioni in esso contenute sul cui rispetto è necessaria la vigilanza del Dirigente e del Responsabile del trattamento. Faccio presente che il regolamento è lo strumento "pubblico", quello cioè che a differenza del D.P.S. (che è documento riservato), deve essere pubblicato affinché tutti ne possano prendere visione.

Regolamento sulla Privacy

Nella Gazzetta Ufficiale n. 11 del 15.1.2007 è stato pubblicato il D.M. n. 305 del 7.12.2006, il Regolamento concernente l'*"identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal MPI, in attuazione dell'art. 20 e 21 del decreto legislativo 30.6.2003 n. 96 (il «Codice in materia di protezione dei dati personali»)"*.

Il Regolamento, predisposto dal MPI, disciplina il trattamento dei dati sensibili e giudiziari gestiti dallo stesso Ministero e dalle istituzioni scolastiche. Si tratta di un quadro generale di garanzie per la gestione dei dati che incidono in modo significativo in particolare sulla sfera privata degli studenti.

Il Regolamento medesimo contiene **una serie di *"schede"*** nelle quali sono riportate le finalità di rilevante interesse pubblico per *"trattare"* i dati sensibili e giudiziari, la relativa fonte normativa,

nonché le operazioni che con i dati si possono eseguire, i tipi di dati utilizzati e la denominazione degli stessi trattamenti.

Scopo del Regolamento è identificare le tipologie dei dati sensibili e giudiziari e delle operazioni indispensabili per la gestione del sistema dell'istruzione. Detti dati devono essere trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei vari casi.

Le varie operazione di trattamento (raffronti, interconnessioni, comunicazioni) sui dati raccolti sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o dei compiti di volta in volta individuati e solo per il perseguimento di rilevanti finalità di interesse pubblico e istituzionale.

Il decreto si sostanzia in sette schede (di seguito, un loro *"riassunto"*).

* * *Scheda 1 - Personale dell'amministrazione e personale scolastico (docenti e ATA)

La *"scheda"* individua tutti i dati che possono essere oggetto di trattamento per le procedure di selezione, di reclutamento, di instaurazione, di gestione e di cessazione del rapporto di lavoro (*dati inerenti lo stato di salute, l'adesione a sindacati, quelli sulle convinzioni religiose per la concessione di permessi legati a particolari festività o per il reclutamento degli insegnanti di religione, i dati sulle convinzioni filosofiche o d'altro genere per eventuali connessioni con lo svolgimento del servizio di leva o come obiettore di coscienza, i dati di carattere giudiziario nell'ambito delle procedure concorsuali che coinvolgono l'interessato, le informazioni sulla vita sessuale connessi unicamente al caso eventuale della rettifica di attribuzione di sesso*); sono individuate, inoltre, le varie tipologie di trattamento possibili.

*** * ***

Scheda 2 - Gestione del contenzioso e procedimenti disciplinari

La *"scheda"* individua il trattamento dei dati sensibili e giudiziari concernente tutte le attività relative alla difesa in giudizio del MPI e delle istituzioni scolastiche nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

* * *

Scheda 3 - Organismi collegiale e commissioni istituzionali

La *"scheda"* individua il trattamento e la descrizione dei dati sensibili nell' ambito degli organismi collegiali e delle commissioni istituzionali, organi rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, che delle famiglie e delle associazioni sindacali. Il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentanti delle organizzazioni sindacali.

* * *

Scheda 4 - Alunni nelle fasi propedeutiche all'avvio dell'anno scolastico

La *"scheda"* individua il trattamento di tutti i dati coinvolti nelle attività propedeutiche all'avvio dell'anno scolastico: si tratta dei dati forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio di ogni ordine e grado re *(è possibile, in tal caso, imbattersi in dati relativi alle origini razziali ed etniche, alle convinzioni religiose, allo stato di salute, alle vicende giudiziarie*).

* * *

Scheda 5 - Alunni nell'attività didattica e nella valutazione

La *"scheda"* attiene al rilevamento e alla trattazione di dati raccolti nell'ambito dell'attività educativa, didattica e formativa e di valutazione (*anche in tal caso possono rilevare i dati sensibili relativi alle origini razziali ed etniche, alle convinzioni religiose, allo stato di salute, ai dati giudiziari, alle convinzioni politiche - per la costituzione e il funzionamento delle Consulte degli studenti*).

* * *

Scheda 6 - Scuole non statali

La *"scheda"* individua i dati sensibili e loro trattamento nel contesto degli Enti vigilati e delle Scuole non statali. Nell'ambito delle procedure di accreditamento e di autorizzazione delle istituzioni scolastiche non statali, l'Amministrazione scolastica periferica esercita attività di: *concessione o revoca della parità; concessione della parifica (scuola primaria); concessione o revoca del riconoscimento legale (scuole secondarie); concessione o revoca della presa d'atto.*

Dati sensibili emergono anche in caso di: *attività di vigilanza e controllo effettuate dall'Amministrazione centrale e periferica che prevedono l'accesso ai fascicoli personali dei docenti e degli alunni.*

Dati sensibili sono, inoltre, trattati dai Dirigenti scolastici nelle scuole dell'infanzia e primarie incaricati della vigilanza sulle scuole non statali.

* * *

Scheda 7 - Rapporti scuola-famiglie: gestione del contenzioso

La *"scheda"* individua i dati sensibili e giudiziari concernenti le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti disciplinari etc.) con gli alunni e con le famiglie.

* * *

Tutte le istituzioni scolastiche dovranno adottare il Regolamento - con delibera formale del Consiglio di Circolo/Istituto - entro il prossimo 28 febbraio.

Allegato	Dimensione
Schede.pdf	815.85 KB
Decreto305.pdf	38 KB

RIFLESSIONI INTORNO AL REGOLAMENTO SUI DATI SENSIBILI E GIUDIZIARI

Dopo una lunga gestazione (legge DL 196 30/06/03 sulla privacy è del 2003) è finalmente stato pubblicato sulla Gazzetta Ufficiale del 15-01-07 il "regolamento sui dati sensibili e giudiziari" (DM 305 del 7/12/06). Ecco alcune riflessioni in proposito.

A COSA SERVE?

Serve ad identificare quali sono i dati sensibili e giudiziari trattabili dall'amministrazione dell'Istruzione (scuole comprese), il tipo di operazioni che con questi dati si possono fare in relazione alle finalità di interesse pubblico perseguite.

Per le Istituzioni scolastiche rappresenta una sorta di strada maestra da percorrere: finché si resta nel tracciato delineato dal Regolamento, il trattamento è legittimo.

ALCUNI PRINCIPI

Il Regolamento definisce uno schema generale di riferimento sui trattamenti effettuabili: quali dati trattati, per quali scopi, le procedure di riferimento. Lo schema del Decreto prevede 3 articoli e 7 schede allegate, dove vengono descritti i trattamenti.

Gli articoli 1 e 2 del Regolamento richiamano più volte il rispetto del principio di indispensabilità del trattamento (i dati vanno trattati solo nella misura strettamente indispensabile alle funzioni da svolgere, in relazione al singolo caso).

LA STRUTTURA DEL REGOLAMENTO

Le schede elencano i trattamenti effettuabili, le operazioni eseguibili, la normativa di riferimento.

Il regolamento e le schede a questo link:
http://isisromero.dyndns.org/regolamenti/regolamenti/regolamento%20privacy.pdf.

I DUBBI

I verbali degli organi collegiali rientrano nella scheda 3 (il cui titolo è proprio "organi collegiali") o nella scheda 5 ("attività educativa, didattica e formativa di valutazione")? La domanda non è retorica, dato che la scheda 3 indica come unico dato sensibile trattabile quello dell'appartenenza ad organizzazioni sindacali.....

IL REGOLAMENTO E IL LAVORO DEI DOCENTI

I docenti, che nella scuola trattano dati sensibili, sono tenuti a conoscere il regolamento.

Utile anche la lettura del "fascicolo informativo" per docenti e personale amministrativo allegato al nostro Documento programmatico sulla sicurezza (sezione "POF e regolamenti" del sito scolastico).

LA PAROLA ALL'AUTORITÀ GARANTE...

Per capire lo "spirito" della legge della privacy seguono alcuni stralci di interviste presenti nel sito http://www.edscuola.com.

Al link http://www.edscuola.com/archivio/software/privacy.htm, una intervista a Francesco Pizzetti, garante della privacy:

DOMANDA: L'impianto normativo che tutela i dati personali ha avuto nelle Pubbliche Amministrazioni un impatto dirompente. . .

RISPOSTA: Vero! Ha costretto le p.a. a riflettere su se stesse e sulla loro organizzazione interna, cosa che una p.a., analogamente ad un soggetto privato, dovrebbe fare costantemente; le ha costrette a verificare se i dati che trattano sono necessari, se sono protetti come il nostro ordinamento giuridico richiede, intendendo l' "ordinamento" inclusivo del patrimonio di civiltà giuridica, ed ha fatto sì che venisse introdotto anche nelle p.a. un livello più alto di rispetto dei cittadini. In fondo proteggere i dati dei cittadini significa tensione costante verso il rispetto e la tutela della loro persona e personalità.

Il punto su cui riflettere è che la tutela della privacy non è solo un problema giuridico, di conformazione alle norme puro e semplice, ma di civiltà anche organizzativa che, per le pp.aa., è una sfida a ripensarsi, trovare con la società un rapporto più moderno ed efficiente.

DOMANDA: Gli adempimenti formali (informativa agli interessati, raccolta dell'eventuale consenso, notifica al Garante) e gli adempimenti organizzativi (modalità di trattamento, conservazione dei dati, articolazione dei ruoli privacy) sono già legge da circa nove anni. Le istituzioni scolastiche agli occhi del Garante in che maniera risultano adempienti e diligenti?

RISPOSTA: Le istituzioni scolastiche risultano essere istituzioni di buona volontà: si interrogano e cercano di tradurre il più possibile queste norme in attività concrete. Anche qui noi dobbiamo essere consapevoli come Authority, che, se parliamo in termini tecnico-giuridici a dei soggetti che hanno una cultura di tipo pedagogico, letterario, storico, matematico, etc., ma non strettamente giuridica, rendiamo meno facile la comprensione dei valori in gioco. Inoltre dobbiamo tener presente il vecchio detto per cui "occorre una generazione per attuare una riforma": oggi certo non è possibile dotarsi di tali tempi, ma comunque bisogna fare i conti con una normativa molto tecnica, che anche a noi crea qualche disorientamento nella sua esplorazione e comprensione causa le infinite sfaccettature. L'importante è:

- che i valori portanti siano capiti è aspetto fondamentale,
- tessere costantemente una rete di confronti tra l'Autorità ed i cittadini, perché può anche darsi che il Legislatore prima e noi di seguito con i provvedimenti che adottiamo configuriamo delle ipotesi di lavoro che poi non risultano concretamente attuabili in un certo tipo di realtà. Questo dialogo è e rimane assolutamente aperto.

Interessante anche questa intervista all'onorevole Paissan, componente della autorità garante della Privacy http://www.edscuola.com/archivio/software/codice_pa.htm :

DOMANDA: On.le Paissan, la legge sulla privacy entrerà in vigore anche nelle scuole dal 1 gennaio 2006. Le scuole sono una pubblica amministrazione un po' particolare. Sono preparate a riceverla?

RISPOSTA: C'è stato un momento di panico nelle scuole, non giustificato; ci sono dei problemi come quello del "portfolio", i dossier di valutazione degli alunni, la loro trasmissione ai gradi successivi delle scuole. E' inutile negare che i problemi sono molto seri, come quello dell'opportunità di trasmettere un certo tipo di informazione, come i rapporti affettivi, la situazione psicologica, etc…, ancorandoli per iscritto per anni ed anni, trasferirli magari anche a scuole private…Abbiamo avviato una serie di valutazioni e confronto con il Miur su questi punti. Le scuole maneggiano dati ed informazioni delicatissime, questa è la circostanza da cui partire, e bisogna che gli operatori scolastici abbiano piena consapevolezza di ciò.Una cosa è che un docente conosca dettagli particolari, privatissimi dello studente e della famiglia mediante colloqui personali, tutt'altra cosa è mettere in forma scritta questi dati, lasciare traccia di situazioni che magari con il tempo si risolvono ed è giusto che cadano nell'oblio.
Questi sono i problemi più grossi da affrontare; affiancati da tutta una serie di questioni più o meno burocratiche che mi preoccupano molto meno".

Ulteriori approfondimenti sono disponibili sul sito della autorità garante http://www.garanteprivacy.it.

IN BUONA SOSTANZA I PESANTI ADEMPIMENTI DEL TRATTAMENTO DEI DATI SENSIBILI E DELLA STESURA DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA RAPPRESENTANO ANCHE UNA OPPORTUNITÀ DI RIFLESSIONE E DI FAR CHIAREZZA

LA PRIVACY NELLE SCUOLE DOPO IL REGOLAMENTO DEL MPI SUL TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI

Premessa

Il 30 gennaio 2007 è entrato in vigore il D.M. del Ministro della Pubblica Istruzione 7 dicembre 2006, n. 305, pubblicato sulla G.U. n. 11 del 15 gennaio 2007: *"Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, in attuazione degli articoli 20 e 21 del Decreto Legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»"* (d'ora in poi "Regolamento").

Il Regolamento innova profondamente la disciplina sul trattamento dei dati sensibili e giudiziari nelle scuole, circoscrivendo i casi in cui è possibile trattare tali dati e specificando le operazioni su di essi eseguibili.
Per comprendere la portata del Regolamento e i motivi della sua adozione, si richiamano innanzitutto i concetti base del trattamento di dati comuni, sensibili e giudiziari nelle scuole, per poi passare alla illustrazione delle previsioni del Regolamento, degli obblighi che ne derivano, delle attività che le scuole devono necessariamente porre in essere per adeguare le attività e i documenti interni (DPS, informative, nomine), degli obblighi di aggiornamento del personale.

Quando è consentito il trattamento dei dati sensibili e giudiziari e perché è stato emanato il regolamento del Ministro della Pubblica Istruzione?

Il Codice Privacy distingue all'interno della categoria dei *"dati personali"*, quelli *"giudiziari"* e *"sensibili"*, definendoli in modo specifico:

- L'articolo 4, Comma 1, lettera d) del Codice definisce **dati sensibili**: *"i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a*

partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale".

- L'articolo 4, Comma 1, lettera e) del Codice definisce **dati giudiziari**: "*i dati personali idonei a rivelare provvedimenti… in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale*".

Rispetto ai dati comuni il Codice della Privacy sottopone il trattamento dei dati **sensibili e giudiziari** a **particolari garanzie** sia in ordine alle modalità di trattamento, sia in relazione al profilo della legittimità formale e sostanziale delle tipologie di dati e delle operazioni che possono essere svolte su di essi.
Infatti, gli artt. 20, Comma 1 e 21, Comma 1 del Codice prevedono che il trattamento dei ***dati sensibili*** e ***giudiziari*** 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;
• le operazioni eseguibili sugli stessi;
• le finalità di rilevante interesse pubblico perseguite.

Gli articoli 20, Comma 2, e 21, Comma 2, del Codice precisano, inoltre, che quando una disposizione di legge abbia specificato le finalità di rilevante interesse pubblico, ma **non i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che su di essi possono essere svolte**, le amministrazioni (nel caso dell'istruzione, il MPI) emanano un APPOSITO REGOLAMENTO, da aggiornare periodicamente, **con il quale identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili**, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dall'articolo 22 del Codice.

G**li effetti del regolamento del** MPI **sull'attività delle scuole**

In applicazione dei sopra richiamati articoli 20 e 21 del Codice Privacy, il Ministero della Pubblica Istruzione.

- ha effettuato, innanzitutto, una preventiva **ricognizione di tutte le attività poste** in essere dalle scuole che comportano un trattamento di dati sensibili o giudiziari;
- ha verificato le **finalità di rilevante interesse pubblico** perseguite dalle scuole in relazione ai compiti ad esse attribuiti dall'ordinamento;
- ha poi valutato l'**indispensabilità dei dati utilizzati** e **delle operazioni svolte** nell'ambito di tali attività **rispetto alle finalità** di volta in volta perseguite;

- ha quindi **emanato un *Regolamento*** (il D.M. 305/2006) con il quale:

• ha individuato gli **ambiti, i processi e i procedimenti** in cui può emergere l'esigenza di trattare dati sensibili e giudiziari;
• ha individuato le **fonti normative** che autorizzano il trattamento e che individuano le **finalità di rilevante interesse pubblico** perseguite;
• ha identificato e reso pubblici i **tipi di dati sensibili e giudiziari utilizzabili e trattabili**;
• ha individuato le **operazioni eseguibili** sui dati sensibili e giudiziari;
• ha specificato i casi in cui è possibile **comunicare i dati** ad altri enti pubblici o a privati.

Vediamo di seguito quali sono le ***conseguenze per l'attività delle scuole***:

- non è consentito il trattamento dei dati sensibili e giudiziari se non per **finalità di rilevante interesse pubblico** individuate dalla Legge e specificate nel Regolamento;
- non è consentito il trattamento dei dati sensibili e giudiziari se non **nell'ambito dei processi/procedimenti individuati nel Regolamento**;
- i dati sensibili e giudiziari **non previsti** dal Regolamento **non possono essere utilizzati e trattati**;
- **non è possibile comunicare** dati sensibili e giudiziari a enti pubblici o privati se non nei **casi previsti dal** R**egolamento**;
- il trattamento in **violazione del** R**egolamento** è **sanzionato penalmente** con la reclusione da sei mesi a tre anni.

Le scuole devono adottare formalmente il regolamento del MPI per il trattamento dei dati sensibili e giudiziari?

Dopo l'emanazione del Regolamento del MPI si è posto il problema se le scuole debbano o meno adottare formalmente il Regolamento tramite delibera del Consiglio di Istituto.
Il Codice parla espressamente di "*atto di **natura regolamentare** adottato in conformità al parere espresso dal Garante … anche su schemi tipo*" (art. 20, Comma 2). Per atto di natura regolamentare si intendono i regolamenti emanati ai sensi dell'art. 17, Commi 3 e 4, della Legge 23 agosto 1988, n. 400, "*adottati previo parere del Consiglio di Stato, sottoposti al visto ed alla registrazione della Corte dei Conti e pubblicati nella Gazzetta Ufficiale*".
In capo ai singoli istituti scolastici manca un potere regolamentare autonomo e dunque, in relazione ai compiti attribuiti al MPI dall'art. 75 Legge 30 luglio 1999, n. 300, **titolare per l'emanazione del regolamento** per il trattamento dei dati sensibili e giudiziari **è il** M**inistro della** P**ubblica** I**struzione.**
Esposte le problematiche in ordine alla natura del Regolamento, va ora chiarito se i Consigli di Istituto debbano formalmente adottare il Regolamento del MPI.

Le scuole, come sopra già evidenziato, non hanno un autonomo potere di emanazione di atti di natura regolamentare e, di conseguenza, non hanno nemmeno il potere di conferire efficacia formale ad atti regolamentari emanati da altri soggetti.

Ne deriva che

il Regolamento per il trattamento dei dati sensibili e giudiziari emanato dal MPI è norma gerarchicamente sovraordinata, produttiva di effetti diretti sulle scuole e, come tale, ***non ha bisogno di alcuna adozione formale*** da parte delle Istituzioni Scolastiche

Che cosa devono fare le scuole in applicazione del Regolamento del MPI?

Dopo aver chiarito cosa le scuole **non devono fare**, elenchiamo sinteticamente che ***cosa le scuole devono fare*** in applicazione del Regolamento del MPI:

Per l'efficacia sostanziale delle previsioni del Regolamento spetta alle scuole la concreta **verifica dell'attuazione delle tutele di ordine procedurale, organizzativo, formativo e informatico** che il Codice prevede debbano accompagnare il trattamento dei dati sensibili e giudiziari. Occorre verificare, ad esempio, che il sistema informativo della scuola consenta un adeguato trattamento dei dati sensibili e giudiziari, in conformità delle previsioni del Codice Privacy e del Regolamento MPI, in ordine alla tipologia dei dati sensibili che è possibile trattare, alle operazioni eseguibili sugli stessi, alle comunicazioni a terzi, alle misure di sicurezza informatica, ecc..

Pertanto, occorre, in primo luogo, **adeguare alle previsioni del** R**egolamento:**

- il Documento Programmatico della Sicurezza. La tenuta di un aggiornato DPS rappresenta una misura minima di sicurezza ai sensi dell'art. 33 e ss. del Codice Privacy. Il Regolamento MPI modifica profondamente le modalità organizzative e operative relative al trattamento di dati sensibili e giudiziari. Pertanto, il mancato adeguamento del DPS alle previsioni del Regolamento rappresenta una violazione dell'obbligo di adozione delle misure minime di sicurezza ed è sanzionato penalmente con l'arresto fino a due anni o con l'ammenda da Euro 10.000 a 50.000 (art. 169 Codice Privacy);
- le informative ex art. 13 del Codice Privacy. Il contenuto delle informative deve essere adeguato al Regolamento, richiamando lo stesso ed evidenziandone i contenuti (il contesto entro cui possono emergere dati sensibili o giudiziari, le tipologie di dati sensibili e giudiziari che possono essere trattati, le modalità del trattamento, le eventuali comunicazioni a terzi degli stessi). L'omessa o inidonea informativa è sanzionata amministrativamente da Euro 3.000 a 18.000;
- i provvedimenti di nomina dei responsabili e degli incaricati per la Privacy nelle scuole, con aggiornamento dei compiti ad essi attribuiti.

È poi necessario ottemperare all'obbligo previsto dall'art. 34, allegato B, del Codice Privacy che prevede **L'OBBLIGATORIETÀ DI INTERVENTI** FORMATIVI degli incaricati del trattamento, per renderli edotti:

• dei rischi che incombono sui dati;
• delle misure disponibili per prevenire eventi dannosi;
• dei **profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività**;
• delle **responsabilità che ne derivano** e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Il citato articolo prevede, altresì, che la formazione deve essere programmata già al momento dell'ingresso in servizio, **nonché in occasione di cambiamenti di mansioni, o di introduzione di *nuovi significativi strumenti*, rilevanti rispetto al trattamento di dati personali.**

Il Regolamento del MPI n. 305/2006 si configura come *nuovo significativo strumento regolativo, rilevante rispetto al trattamento di dati personali* e, pertanto, i D**irigenti** S**colastici**, in qualità di *Titolari del trattamento dei dati* e in base alle previsioni del richiamato art. 34, allegato B del Codice Privacy, ***devono organizzare momenti formativi*** **per aggiornare il personale scolastico** (docenti e personale ATA):

• **sui contenuti del** R**egolamento;**
• **sui conseguenti rischi di natura sanzionatoria** (penali, civili, amministrativi) e **organizzativa** (gestione dei procedimenti e dei processi ove emergono dati sensibili e giudiziari e delle relative banche dati);
• **sulle modalità di adeguamento al** R**egolamento:** del DPS; **delle informative** ex art. 13 Codice Privacy; delle **nomine e dei compiti** degli incaricati e dei responsabili Privacy;
• sull'**impatto della nuova disciplina sui sistemi informatici** e sulle **banche dati**, sulle **misure di sicurezza tecnico-informatiche da adottare per prevenire i rischi di trattamento illecito dei dati sensibili e giudiziari.**

L'adempimento degli obblighi di formazione, oltre ad assicurare al personale scolastico la necessaria informazione per gestire efficacemente i processi della Privacy alla luce del Regolamento MPI, consente di **regolarizzare la posizione dei** D**irigenti** S**colastici** nei confronti degli **obblighi formativi** scaturenti dal combinato disposto degli artt. da 33 a 36 del Codice e del punto 19.6 dell'All. B (disciplinare tecnico), e di limitare il rischio rispetto ai rilevanti profili di responsabilità e sanzionatori che ne possono derivare e che di seguito si illustrano:

- l'obbligo di formazione deve trovare una sua pianificazione nel DPS e, dunque, l'attività formativa si configura come "misura minima di sicurezza" (vedi punto 19.6 disciplinare tecnico); **l'omessa formazione** può quindi delineare, *in via diretta* ed autonomamente, una **violazione dell'obbligo di adozione di misure minime di sicurezza** previsto dall'art. 33 del Codice Privacy, **sanzionabile con l'arresto** fino a due anni o con l'ammenda da Euro 10.000 a 50.000 (art. 169 Codice Privacy);

- la mancata attivazione di momenti formativi potrebbe essere valutata come un indicatore di **responsabilità civilistica** del "datore di lavoro-Dirigente Scolastico", ad esempio in sede di giudizio per trattamento illecito di dati sensibili da parte di un incaricato (docente, ATA). In tal caso, in applicazione delle norme del Codice Privacy (art. 15, che richiama l'art. 2050 del Codice Civile(1)) e delle altre norme in materia di risarcimento del danno:
  - **per l'incaricato** che ha direttamente commesso l'illecito si applicherebbe l'art. 2050 C.C. e, quindi, la sanzione civile del risarcimento del danno, se l'incaricato non prova di *avere adottato tutte le misure idonee a evitare il danno* (oltre alla applicazione delle sanzioni penali, se ne ricorrono le condizioni);
  - **in capo al** D**irigente** S**colastico**, può configurarsi una doppia responsabilità:

A) una **responsabilità civile oggettiva** in applicazione **dell'art. 2049** del Codice Civile (*Responsabilità dei padroni e dei committenti*) in base al quale il datore di lavoro [il Dirigente Scolastico] risponde dei danni arrecati dai suoi dipendenti a titolo di responsabilità per fatto altrui, a prescindere dai profili di una concreta "c*ulpa in eligendo o in vigilando*" dello stesso datore di lavoro(2);

B) una responsabilità ai sensi **dell'art. 2050 C.C.** per **non avere adottato** nella struttura da lui diretta **tutte le misure idonee a evitare il danno.**

Nel caso A) - *responsabilità oggettiva* - l'omessa formazione del personale in materia di Privacy potrebbe essere una delle cause - se non la causa diretta - del comportamento illecito del personale scolastico per mancata conoscenza degli aspetti normativi, operativi e tecnici; ***è, quindi, interesse del Dirigente Scolastico fornire ai suoi collaboratori un adeguato aggiornamento per evitare che possano commettere illeciti*** e ***danni per i quali potrebbe essere chiamato a rispondere direttamente***: un personale aggiornato sugli aspetti normativi, operativi e tecnici ha senz'altro minori possibilità di commettere illeciti in sede di trattamento di dati personali rispetto ad altro personale non adeguatamente informato e aggiornato.

Nel caso B) *- responsabilità per non avere adottato misure idonee ad evitare il danno* - l'**attività di formazione** del personale, essendo prevista da Codice Privacy come obbligatoria, può **essere considerata una misura idonea ad evitare il danno**; la mancata attività di aggiornamento del personale, quindi, potrebbe benissimo configurarsi come omessa adozione di una delle misure idonee a evitare il danno.
Considerate, inoltre, le cautele che circondano il trattamento di dati sensibili e giudiziari, appare assolutamente consigliabile l'attivazione di corsi di aggiornamento sui contenuti e sugli effetti del Regolamento del MPI.

(1) Art. 2050 C.C: "Responsabilità per l'esercizio di attività pericolose. 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 avere adottato tutte le misure idonee a evitare il danno."
(2) Cassazione, sentenza 89/2002.PAISVI

Ricapitolando

ILTRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI NELLE SCUOLE DOPO L'EMANAZIONE DEL REGOLAMENTO DELMINISTRODELLAPUBBLICAISTRUZIONE (D.M. 305/2006)

Il 7 dicembre 2006 il MPI ha emanato il **REGOLAMENTO sul trattamento dei dati sensibili e giudiziari** (D.M. 305/2006, entrato in vigore il 30 gennaio 2007).

Perché un Regolamento del MPI?

Il Regolamento individua i tipi di dati **sensibili e giudiziari** e le **operazioni eseguibili** su di essi e **legittima il trattamento di tali dati** da parte delle scuole;

Le scuole devono formalmente adottare il Regolamento?

Il Regolamento **è immediatamente applicabile e NON richiede una formale adozione da parte dei Consigli di Istituto delle scuole**. Le scuole devono, invece, dare concreta attuazione alle tutele di ordine procedurale, organizzativo e informatico previste dal Codice Privacy in ordine al trattamento dei dati sensibili e giudiziari.

Il Regolamento MPI e le principali CONSEGUENZE PER LE SCUOLE

- non è consentito il trattamento dei dati sensibili e giudiziari se non per le **finalità di rilevante interesse pubblico** individuate dalla legge e specificate nel Regolamento MPI;
- non è consentito il trattamento dei dati sensibili e giudiziari se non **nell'ambito dei processi/procedimenti individuati nel Regolamento;**
- i dati sensibili e giudiziari non previsti dal Regolamento **non possono essere utilizzati e trattati**; l'eventuale **consenso dell'interessato** all'esecuzione di operazioni su dati sensibili e giudiziari non previsti nel Regolamento **non legittima il trattamento stesso**;
- **non è possibile comunicare** dati sensibili e giudiziari a enti pubblici o privati se non nei **casi previsti dal Regolamento**;

- il **trattamento in violazione del** R**egolamento è sanzionato penalmente** con la **reclusione** da sei mesi a tre anni;
- le novità introdotte dal Regolamento MPI richiedono:

* l'aggiornamento del D**ocumento** P**rogrammatico della** S**icurezza** (il non aggiornamento è sanzionato penalmente con l'arresto fino a due anni o con l'ammenda da Euro 10.000 a 50.000);
* l'aggiornamento delle **informative ex art. 13 del** C**odice** P**rivacy** (l'omessa o inidonea informativa è sanzionata amministrativamente da Euro 3.000 a 18.000);
* l'adeguamento dei **provvedimenti di nomina** dei responsabili e degli incaricati per la Privacy nelle scuole, con aggiornamento dei compiti ad essi attribuiti;
*** l'attivazione di** INTERVENTI FORMATIVI degli incaricati del trattamento.

L'omessa formazione:

a) configura una violazione delle misure minime di sicurezza ed è quindi sanzionata anche penalmente;
b) può delineare profili di responsabilità civile con obbligo di risarcimento del danno per il Dirigente Scolastico, ai sensi dell'art. 2049 C.C. (responsabilità oggettiva, in caso di comportamenti illeciti del personale riconducibili all'omessa formazione) e 2050 C.C. (per mancata adozione di tutte le misure, anche formative, idonee ad evitare il danno).

I CONTENUTI DEL REGOLAMENTO DEL MPI

Il Regolamento del MPI è strutturato in ***schede*** allegate ad un breve articolato introduttivo (vedi schema-tipo fig. 1).

Le ***schede*** riportano:

- l'"**indicazione del trattamento e la descrizione riassuntiva del contesto**";
- le "**finalità di rilevante interesse pubblico**" perseguite dal trattamento, con indicazione delle norme del Codice Privacy dalle quali è possibile trarre un rilevante interesse pubblico;
- le "**fonti normative**" che autorizzano il trattamento (il trattamento dei dati sensibili e giudiziari può essere effettuato se previsto da una norma e quindi il Regolamento individua puntualmente le fonti normative);
- i "**tipi di dati sensibili trattati**" e cioè le informazioni che consentono di individuare, l'origine razziale o etnica, le convinzioni religiose, sindacali, politiche, lo stato di salute, la vita sessuale, i dati di carattere giudiziario;
- le "**operazioni eseguibili**", con riferimento:
- a quelle possibili in **via ordinaria** (***particolari forme di trattamento***): operazioni di natura informatica relative a interconnessioni e raffronti di dati; **comunicazioni a terzi**; diffusione tramite pubblicazioni in varia forma;
- alle ***altre tipologie più ricorrenti di trattamenti*** (raccolta presso interessati o presso terzi; elaborazioni cartacee o con modalità informatizzate; altre operazioni indispensabili rispetto ai fini del trattamento e diverse da quelle "ordinarie" quali registrazione, conservazione, consultazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione interna, cancellazione).

Fig. 1: schema-tipo delle schede allegate al regolamento del MPI

INDICAZIONE DEL TRATTAMENTO E DESCRIZIONE RIASSUNTIVA DEL CONTESTO
FINALITÀ DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
FONTI NORMATIVE
TIPI DI DATI TRATTATI
• ORIGINE ☐ razziale ☐ etnica • CONVINZIONI ☐ religiose ☐ filosofiche ☐ d'altro genere • CONVINZIONI ☐ politiche ☐ sindacali • STATO DI SALUTE ☐ patologie attuali ☐ patologie pregresse ☐ terapie in corso ☐ anamnesi familiare • VITA SESSUALE ☐ • DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e), del Codice) ☐
OPERAZIONI ESEGUITE
Particolari forme di trattamento
Altre tipologie più ricorrenti di trattamenti
• RACCOLTA: ☐ presso gli interessati ☐ presso terzi • ELABORAZIONE: ☐ in forma cartacea ☐ con modalità informatizzate • Altre operazioni indispensabili rispetto ai fini del trattamento e diverse da quelle *"ordinarie":*

La complessità dei processi di lavoro e dei procedimenti che possono richiedere il trattamento di dati sensibili e giudiziari ha suggerito la redazione di più schede (sette) riferire ai seguenti ambiti:

- ***Scheda 1:*** Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro;
- ***Scheda 2:*** Gestione del contenzioso e procedimenti disciplinari;
- ***Scheda 3:*** Organismi collegiali e commissioni istituzionali;
- ***Scheda 4:*** Attività propedeutiche all'avvio dell'anno scolastico;
- ***Scheda 5:*** Attività educativa, didattica e formativa, di valutazione;
- ***Scheda 6:*** Scuole non statali;
- ***Scheda 7:*** Rapporti scuola-famiglie: gestione del contenzioso.

Per quanto riguarda l'ambito della *"Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro" (scheda 1)*, nel Regolamento, considerata l'unitarietà dei processi di lavoro e di alcuni riferimenti normativi, la scheda è riferita sia al personale della scuola, sia a quello amministrativo del MPI e a quello dell'AFAM. In ogni scheda è stata invece differenziata la sezione relativa alle fonti normative, articolata in:
• norme comuni;
• norme relative al personale amministrativo del MPI;
• norme per il personale delle Istituzioni Scolastiche;
• norme per il personale AFAM.

Sulla base del contenuto delle Schede allegate al Regolamento MPI, nei quadri sinottici che seguono si schematizzano i diversi ambiti e processi di lavoro, con indicazione del contesto entro cui possono emergere dati sensibili e giudiziari e del relativo trattamento.

REGOLAMENTO DELMPI (D.M. 305/2006): PROCESSI GESTITI DALLE SCUOLE E INDICAZIONI SULTRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI

Processo gestito	Contesto entro cui possono emergere dati sensibili e giudiziari e indicazione del trattamento
Scheda 1 **Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro:** • **del personale dipendente dell'Amm.ne Centrale e Periferica del MPI, e Dirigente, docente, educativo ed ATA delle Istituzioni Scolastiche ed educative, personale IRRE;** • **dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato**	*Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro.* ➢ I dati inerenti lo **stato di salute** sono trattati per: l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative, pensionistiche e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale; ➢ I dati idonei a rilevare **l'adesione a sindacati** o ad organizzazioni di carattere sindacale ai fini degli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali; ➢ I dati sulle **convinzioni religiose** per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione; ➢ I dati sulle **convinzioni filosofiche** o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza; ➢ I dati di **carattere giudiziario** sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato; ➢ le informazioni sulla **vita sessuale** possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.

Scheda 2
Gestione del contenzioso e procedimenti disciplinari

Il trattamento dei dati sensibili e giudiziari concerne tutte le attività relative alla **difesa in giudizio** del Ministero dell'Istruzione e delle Istituzioni Scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

Scheda 3
Organismi Collegiali e Commissioni Istituzionali

- Il trattamento dei dati sensibili è necessario per attivare gli Organismi Collegiali e le Commissioni Istituzionali previsti dalle norme di organizzazione del Ministero della Pubblica Istruzione e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali;
- Il dato sensibile trattato è quello **dell'appartenenza alle organizzazioni sindacali**, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentanti delle organizzazioni sindacali**.**

Scheda 4
Attività propedeutiche all'avvio dell'anno scolastico

I dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio nelle Istituzioni Scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.

Nell'espletamento delle attività propedeutiche all'avvio dell'anno scolastico da parte delle Istituzioni Scolastiche, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche, per favorire **l'integrazione degli alunni** con cittadinanza non italiana;
- alle convinzioni religiose, per garantire la **libertà di credo religioso** e per la fruizione dell'**insegnamento della religione cattolica** o delle **attività alternative** a tale insegnamento;
- allo stato di salute, per assicurare l'erogazione del **sostegno agli alunni diversamente abili** e per la **composizione delle classi**;
- alle vicende giudiziarie, per assicurare il **diritto allo studio** anche a soggetti sottoposti a regime di detenzione; i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un **programma di protezione** nei confronti dell'alunno nonché nei confronti degli alunni che abbiano commesso reati.

Scheda 5
Attività educativa, didattica e formativa, di valutazione

*Nell'espletamento delle **attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami,** da parte delle Istituzioni Scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali, possono essere trattati dati sensibili relativi:*

- alle **origini razziali ed etniche** per favorire l'integrazione degli alunni con cittadinanza non italiana;
- alle **convinzioni religiose** per garantire la libertà di credo religioso;
- allo **stato di salute**, per assicurare l'erogazione del servizio di **refezione scolastica**, del **sostegno** agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da **gravi patologie**, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle **visite guidate e ai viaggi di istruzione**;
- ai **dati giudiziari,** per assicurare il diritto allo studio anche a soggetti sottoposti a **regime di detenzione**;
- alle **convinzioni politiche**, per la costituzione e il funzionamento delle **Consulte** e delle **Associazioni** degli studenti e dei genitori;
- I dati sensibili possono essere trattati per le **attività di valutazione** periodica e finale, per le attività di **orientamento** e per la compilazione della **certificazione delle competenze**.

Scheda 6
Scuole non statali

Nell'ambito delle procedure di accreditamento e autorizzazione delle Istituzioni Scolastiche non statali, l'Amministrazione Scolastica periferica esercita attività di: concessione o revoca della parità; concessione della parifica (scuola primaria); concessione o revoca del riconoscimento legale (scuole secondarie); concessione o revoca della presa d'atto.

Dati sensibili emergono nel caso di **attività di vigilanza e controllo** effettuate dall'Amministrazione centrale e periferica che prevedono l'accesso ai fascicoli personali dei docenti e degli alunni.

Dati sensibili sono, inoltre, **trattati dai** D**irigenti** S**colastici** delle scuole dell'infanzia e primarie **incaricati della vigilanza sulle scuole non statali provviste di autorizzazione**.

Scheda 7
Rapporti scuola-famiglie: gestione del contenzioso

Il trattamento di dati sensibili e giudiziari concerne tutte le attività connesse alla instaurazione di **contenzioso** (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'Autorità Giudiziaria, etc.) **con gli alunni e con le famiglie**, e tutte le attività relative alla **difesa in giudizio** delle Istituzioni Scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.

Informazione al Collegio docenti da parte del Dirigente scolastico

Il Dirigente scolastico informa il collegio dell'emanazione, con Decreto Ministeriale n.305 del 7.12.2006, del **Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione**. Il Regolamento completa il quadro normativo relativo al diritto alla protezione dei dati personali ed alla riservatezza definito dal codice emanato con il D.lgs 196 del 30 giugno 2003. Il Codice è entrato in vigore il 1° gennaio 2004 ed ha riunito in modo organico la normativa di tutela relativa al trattamento dei dati personali; ha offerto all'intera amministrazione pubblica un'occasione significativa per portare a compimento il processo di modernizzazione, in modo da adeguare il proprio assetto organizzativo e funzionale dando idonee risposte alle istanze dei cittadini rivolte al massimo rispetto dei diritti e delle libertà fondamentali. Nella scuola abbiamo provveduto a dare attuazione al codice per quanto riguarda le autorizzazioni al trattamento dei dati personali al personale coinvolto, attraverso gli incarichi conferiti al personale docente da parte del dirigente scolastico ed al personale ATA (assistenti amministrativi e collaboratori scolastici) da parte del Responsabile del trattamento (Direttore dei servizi generali e amministrativi); ogni incarico è stato corredato di linee guida contenete istruzioni per il trattamento e la protezione dei dati; è stato fornita l'informativa dei diritti ai soggetti interessati (personale, alunni e genitori e fornitori); sono state definite e vengono applicate e monitorate le misure minime di sicurezza dei dati; è stato stilato il Documento Programmatico sulla sicurezza il cui aggiornamento è stato effettuato in data……

Il Decreto Ministeriale, che regola il trattamento dei dati sensibili e giudiziari nel settore dell'istruzione, è un provvedimento importante, previsto dagli articoli 20 e 21 del D.lgs 196/03 ed è stato più volte sollecitato dal Garante per la protezione della privacy. Il Regolamento specifica i tipi di dati che possono essere

trattati dalla scuole, le operazioni che su di essi sono eseguibili e le finalità di rilevante interesse pubblico perseguite.

Il testo del Regolamento è suddiviso in 3 articoli nei quali si richiama il D.lgs 196/03 e si sottolinea, nell'art. 2, **l'obbligo di trattare dati sensibili e giudiziari solo previa verifica della loro pertinenza, completezza e indispensabilità** rispetto alle finalità perseguite nei singoli casi, specie quando la raccolta non avvenga presso l'interessato. Il dirigente invita quindi i docenti a non richiedere e a non trattare dati personali degli alunni e delle famiglie che non siano necessari effettivamente alle attività e che siano invece motivati da una mera volontà di conoscenza delle situazioni personali, di salute o familiari degli alunni.

Il dirigente illustra le **7 schede che sono parte integrante del Regolamento** e che individuano tutti i dati sensibili e giudiziari trattati dalle scuole, suddividendoli in 6 macro-categorie (ambiti):
Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;
Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari;
Scheda n. 3 – Organismi collegiali e commissioni istituzionali;
Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico;
Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione;
Scheda n. 6 – Scuole non statali (relativamente agli eventuali dati sensibili e giudiziari che emergono nell'attività di vigilanza e controllo effettuata dall'Amministrazione e dai dirigenti scolastici delle scuole primarie incaricati della vigilanza sulle scuole non statali autorizzate);
Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.

In particolare nella scheda n.4 relativa alle "Attività propedeutiche all'avvio dell'anno scolastico" si precisa che i dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.
Nell'espletamento delle attività propedeutiche all'avvio dell'anno scolastico da parte delle istituzioni scolastiche, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana; alle convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione

dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- allo stato di salute, per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi;
- alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
- i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno nonché nei confronti degli alunni che abbiano commesso reati.

Nella scheda n. 5 relativa alla "Attività educativa. didattica e formativa, di valutazione" si precisa che nell'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, da parte delle istituzioni scolastiche dì ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche per favorire l'integrazione degli alunni con cittadinanza non italiana;
- alle convinzioni religiose per garantire la libertà di credo religioso;
- allo stato di salute, per assicurare 1'erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;
- ai dati giudiziari, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
- alle convinzioni politiche, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori,

I dati sensibili possono essere trattati per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze.

Ogni scheda consente alle scuole di individuare chiaramente i trattamenti consentiti, le finalità di rilevante interesse pubblico perseguite, le fonti normative, i soggetti esterni pubblici e privati a cui è possibile comunicare i dati, i tipi di dati trattati e le tipologie più ricorrenti di trattamento.

Nel Documento Programmatico per la Sicurezza della scuola la sezione relativa all'elenco dei dati personali trattati (punto 19.1 del Disciplinare tecnico) sarà adeguata alle prescrizioni e indicazioni contenute nelle schede. A breve sarà riformulata e adeguata la nomina del Responsabile del Trattamento, richiamando le prescrizioni contenute nel Regolamento; il Responsabile, a sua volta, provvederà ad effettuare le nomine degli incaricati del trattamento, modificando secondo gli indirizzi e le indicazioni fornite le autorizzazioni concesse. Gli incarichi del dirigente scolastico, relativi al personale docente, saranno consegnati individualmente. La presente comunicazione vale come autorizzazione provvisoria per tutti i docenti della scuola. L'informativa agli interessati verrà effettuata nuovamente facendo riferimento alle prescrizione del Regolamento e la diffusione della sua conoscenza, effettuata fra i docenti con la presente comunicazione, sarà oggetto di una specifica occasione di formazione per il personale ATA incaricato.

In questa occasione sono state fornite le informazioni necessarie e l'autorizzazione al trattamento dei dati da parte dei docenti della scuola i quali sono pertanto autorizzati a trattare i dati sensibili e giudiziari nel contesto definito dalle schede allegate al decreto e nel rispetto delle finalità di rilevante interesse pubblico perseguite, precisate dalle schede:

* n. 4 Attività propedeutiche all'avvio dell'anno scolastico

* n. 5 Attività educativa, didattica e formativa e di valutazione e
* n. 6 Rapporti Scuola-Famiglie: gestione del contenzioso

(limitatamente ai casi nei quali sono fossero coinvolti).
I docenti potranno trattare i tipi di dati indicati dalle schede citate e potranno effettuare le operazioni consentite in esse elencate e le tipologie più ricorrenti di trattamenti. Il dirigente informa che le schede citate saranno affisse all'albo docenti, messe a disposizione in sala docenti e pubblicate sul sito della scuola. Tutti i docenti hanno l'obbligo di prendere visione del Documento Programmatico per la Sicurezza e attenersi ad esso. Il Documento sarà aggiornato entro il 30 marzo prossimo e, entro tale data, affisso nuovamente all'albo e pubblicato sul sito della scuola. Il dirigente scolastico informa i docenti, facendo riferimento alle schede allegate al decreto n. 1, 2 e 3 in quali modi sono trattati dalla scuola i dati sensibili e giudiziari del personale.

Informativa per web (esempio tratto dal sito di una scuola)

IPSIA GALILEI rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono a IPSIA GALILEI. In generale, l'utente può navigare sul sito web dell'IPSIA GALILEI senza fornire alcun tipo di informazione personale. La raccolta ed il trattamento di dati personali avvengono quando necessarie a IPSIA GALILEI in relazione all'esecuzione di servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tali circostanze, la presente politica della privacy illustra le modalità ed i caratteri di raccolta e trattamento dei dati personali dell'utente. IPSIA GALILEI tratta i dati personali forniti dagli utenti in conformità alla normativa vigente.

Raccolta di Dati Personali
Dati personali significa qualsiasi informazione che possa essere impiegata per identificare un individuo, una società od altro ente. A titolo puramente esemplificativo e non esaustivo viene raccolto ad esempio il nome ed il cognome, l'indirizzo di posta elettronica (e-mail), l'indirizzo, un recapito postale od altro recapito di carattere fisico, altre informazioni necessarie per contattare l'utente, qualifica, data di nascita, genere, lavoro, attività commerciale, interessi personali, altre informazioni necessarie per la prestazione di servizi richiesti dall'utente.

La navigazione sul sito dell'IPSIA GALILEI avviene in forma anonima, a meno che l'utente abbia precedentemente specificato che desidera che IPSIA GALILEI ricordi l'identificativo con cui si è registrato e la relativa password. IPSIA GALILEI non compie operazioni di raccolta dati dell'utente con modalità automatiche, incluso l'indirizzo di posta elettronica (e-mail). IPSIA GALILEI registra l'indirizzo IP dell'utente (Internet Protocol, vale a dire l'indirizzo Internet del computer dell'utente) per avere un'idea dell'area del sito che l'utente visita e della durata della visita, nel rispetto della normativa vigente in tema di tutela di dati personali. Tuttavia, IPSIA GALILEI non mette in relazione l'indirizzo IP dell'utente con altre informazioni personali relative allo stesso se non dopo averlo debitamente informato del relativo trattamento ed avere ottenuto il suo consenso al trattamento, e solo rispetto ad utenti registrati al sito dell'IPSIA GALILEI. Come molti altri siti web aventi carattere e contenuto indirizzato ai servizi, il sito dell'IPSIA GALILEI può impiegare una tecnologia standard chiamata "cookie" per raccogliere informazioni sulle modalità di uso del sito da parte dell'utente. Per ulteriori informazioni, l'utente è invitato a consultare la seguente sezione "Cookies ".

L’IPSIA GALILEI raccoglie i dati personali dell'utente in occasione della sua registrazione all’IPSIA GALILEI, per emettere un account, necessario all’utente per usufruire di determinati prodotti o servizi dell’IPSIA GALILEI.
In particolare la registrazione è necessaria all'utente per partecipare al forum, per usufruire della chat, per poter inviare messaggi ad altri iscritti, per inserire commenti alle notizie, quando l'utente chiede di ricevere determinate e-mails o di essere inserito in una mailing list, o quando l'utente, per qualsiasi altra ragione, comunica i propri dati personali a IPSIA GALILEI. IPSIA GALILEI usa tali informazioni solamente ove le stesse siano state legittimamente raccolte, in conformità alla presente Politica della Privacy e nel rispetto della normativa vigente.

Comunicazione di Dati Personali
In caso di raccolta di dati personali, IPSIA GALILEI informerà l'utente delle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente. IPSIA GALILEI non comunicherà i dati personali dell'utente a terzi senza il consenso dell'utente, salvo le limitate circostanze specificate in seguito nella Sezione "Ambito di Comunicazione e Diffusione di Dati Personali".

Se l'utente decide di fornire a IPSIA GALILEI i propri dati personali, IPSIA GALILEI potrà comunicarli all'interno dell'Istituto dell’IPSIA GALILEI od a terzi che prestano servizi a IPSIA GALILEI, solo rispetto al coloro che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente. IPSIA GALILEI invierà all'utente materiale relativo ad attività di informazione ed a ricerche di mercato solo dopo aver informato l'utente ed aver ottenuto il consenso dello stesso al trattamento, in conformità alle disposizioni vigenti in tema di protezione di dati personali.

Cookies
Un cookie è un piccolo file di testo che alcuni siti web inviano all'hard drive dell'utente in occasione della visita al sito. Un cookie può contenere informazioni quali un ID dell'utente che il sito usa per controllare le pagine visitate, ma le uniche informazioni di carattere personale che un cookie può contenere sono quelle fornite dall'utente stesso. Un cookie non può leggere i dati presenti sull'hard disk dell'utente o leggere i cookies creati da altri siti. Alcune aree del sito web di IPSIA GALILEI impiegano cookies per registrare le modalità di navigazione degli utenti sul sito. IPSIA GALILEI si serve di cookies per determinare il grado di utilità delle informazioni che fornisce ai propri utenti e per verificare l'efficacia della struttura di navigazione del sito in relazione al supporto aiuto offerto all'utente per ottenere quell'informazione.
Se l'utente non desidera ricevere cookies durante la navigazione sul sito di IPSIA GALILEI, può programmare il proprio browser in modo da essere avvertito prima di accettare cookies e rifiutare i cookies quando il browser avvisa della presenza di cookies. L'utente può anche rifiutare tutti i cookies disattivandoli nel proprio browser, anche se in tal modo l'utente non sarebbe poi in grado di beneficiare in pieno dei vantaggi del sito dell’IPSIA GALILEI. In particolare, all'utente potrebbe essere chiesto di accettare cookies al fine di compiete determinate operazioni sul sito web di IPSIA GALILEI. Tuttavia, non è

necessario che l'utente accetti tutti i cookies per usare /navigare in molte aree del sito di IPSIA GALILEI, salvo il caso in cui per l'accesso a specifiche pagine web di IPSIA GALILEI siano necessari la registrazione ed una password.

Finalità e Modalità di Trattamento dei Dati Raccolti
IPSIA GALILEI tratta i dati personali dell'utente per le seguenti finalità di carattere generale: per soddisfare le richieste relative a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito, per aggiornare l'utente sulle ultime novità in relazione ai servizi dell'IPSIA GALILEI, od altre informazioni che IPSIA GALILEI ritiene siano di interesse dell'utente, e che provengono da IPSIA GALILEI o dai suoi partners, e per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori. Il trattamento di dati personali dell'utente da parte dell'IPSIA GALILEI per le finalità sopra specificate avviene in conformità alla normativa vigente a tutela di dati personali.

Ambito di Comunicazione e Diffusione di Dati Personali
I dati personali dell'utente non vengono comunicati al di fuori della realtà dell'IPSIA GALILEI senza il consenso dell'interessato, salvo quanto di seguito specificato.
Nell'ambito dell'organizzazione dell'IPSIA GALILEI, i dati sono conservati in servers controllati cui è consentito un accesso limitato in conformità alla normativa vigente a tutela di dati personali.

IPSIA GALILEI può comunicare i dati personali dell'utente a terzi in uno dei seguenti casi: quando l'interessato abbia prestato il proprio consenso alla comunicazione; quando la comunicazione sia necessaria per fornire il prodotto od il servizio richiesto dall'utente; la comunicazione sia necessaria in relazione a terzi che lavorano per conto dell'IPSIA GALILEI per fornire il prodotto od il servizio richiesto dall'utente (IPSIA GALILEI comunicherà a questi solo le informazioni che si rendono necessarie in relazione alla prestazione del servizio, ed alle stesse è vietato trattare i dati per finalità diverse); o per fornire all'utente le informazioni che IPSIA GALILEI ritenga sia interessato a conoscere dall'IPSIA GALILEI stessa e dagli altri enti ad essa collegati (in qualsiasi momento l'utente potrà richiedere di non ricevere più tale tipo di informazioni). IPSIA GALILEI inoltre divulgherà i dati personali dell'utente in caso ciò sia richiesto dalla legge.

Diritti dell'Utente; User Account
Se l'utente è un utente è registrato, lo stesso può avere accesso ai propri dati personali accedendo alla pagina in cui sono contenuti dalla voce di menù "Il mio PROFILO". L'utente può chiedere la cancellazione dalla newsletter, può limitare la diffusione delle propria email o in generale del proprio profilo agli altri iscritti. Per chiedere la cancellazione del proprio IPSIA GALILEI account o qualsiasi altro proprio dato personale inviando un'e-mail al seguente indirizzo: …….

Sicurezza dei Dati
Le informazioni del IPSIA GALILEI account dell'utente sono protette da una password per garantire la riservatezza e la sicurezza dell'utente. IPSIA GALILEI

adotta tutte le misure di sicurezza e le procedure fisiche, elettroniche, ed organizzative richieste dalla normativa vigente, In alcune aree del proprio sito web, IPSIA GALILEI impiega sistemi standard SSL di criptazione per aumentare la sicurezza della trasmissione di dati. Anche se IPSIA GALILEI fa quanto ragionevolmente possibile per proteggere i dati personali dell'utente, IPSIA GALILEI non può garantire la completa totale sicurezza dei dati trasmessi dagli utenti durante la comunicazione, quindi l'IPSIA GALILEI invita calorosamente l'utente ad adottare tutte misure precauzionali per proteggere i propri dati personali quando navigano su Internet. Ad esempio, l'utente è invitato a cambiare spesso la propria password, usare una combinazione di lettere e numeri, ed assicurarsi di fare uso di un browser sicuro.

I Minori e la Privacy
Il sito web dell'IPSIA GALILEI è pensato per un utilizzo anche da parte di minori di 18 anni in quanto presenta contenuti puramente didattici e culturali. Quindi IPSIA GALILEI non richiede, in fase di iscrizione, la maggiore età dell'utente..

Siti di Terzi
Il sito web dell'IPSIA GALILEI contiene links ad altri siti. IPSIA GALILEI non condivide i dati personali dell'utente con questi siti e non è responsabile delle pratiche degli stessi in relazione alla tutela ed al trattamento di dati personali. IPSIA GALILEI invita l'utente a prendere visione delle politiche della privacy di tali siti per conoscere le modalità di trattamento e raccolta dei propri dati personali da parte di tali siti web di terzi.

Modifiche alla politica della Privacy
IPSIA GALILEI modificherà di volta in volta la presente politica della Privacy. Qualora IPSIA GALILEI modifichi in termini sostanziali le modalità di trattamento dei dati personali dell'utente, renderà disponibile tale informazione pubblicando apposita comunicazione sul proprio sito.

Domande o Suggerimenti
In caso di domande o dubbi in relazione alla raccolta, all'uso al trattamento, od alla comunicazione o diffusione dei propri dati personali, l'utente può inviare un'e-mail al seguente indirizzo di posta elettronica:
……
Il presente documento è stato aggiornato il …….

Adozione regolamento Privacy – Documento Programmatico Sicurezza

IL CONSIGLIO DI CIRCOLO

PREMESSO CHE Il Codice in materia di protezione dei dati personali, emanato con il Decreto legislativo 30 giugno 2003, n. 196 ed entrato in vigore il 1° gennaio 2004, ha riunito in modo organico la normativa di tutela relativa al trattamento dei dati personali ed ha offerto all'intera amministrazione pubblica un'occasione significativa per portare a compimento il processo di modernizzazione, in modo da adeguare il proprio assetto organizzativo e funzionale dando idonee risposte alle istanze dei cittadini rivolte al massimo rispetto dei diritti e delle libertà fondamentali.
In attuazione del D. Lgs 196/2003 ed in ottemperanza delle prescrizioni dell'Autorità Garante della Privacy contenute nel Comunicato stampa del 18 luglio 2005, con D.M. n. 305 del 7 dicembre 2006, pubblicato nella Gazzetta Ufficiale n. 11 del 15.1.2007, il Ministero della Pubblica Istruzione ha provveduto alla stesura del "*Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione dell'art. 20 e 21 del decreto legislativo 30 giugno 2003"*, individuando le garanzie da osservare in ordine al trattamento di alcune informazioni che riguardano profili particolarmente delicati della sfera privata delle persone.
Data la grande rilevanza di tale Decreto emerge dallo stesso dettato del Comunicato stampa del Garante, secondo il quale: *in assenza di atti di natura regolamentare "il trattamento dei dati sensibili e giudiziari dovrà essere interrotto". La prosecuzione del trattamento dei dati risulterebbe, infatti, illecita, con conseguenti responsabilità anche di ordine contabile e per danno erariale. E potrebbe, inoltre, comportare l'inutilizzabilità dei dati trattati indebitamente e il possibile intervento di provvedimenti anche giudiziari di blocco o di divieto del trattamento.*
VISTA la necessità della predisposizione di un vero e proprio Regolamento da parte del MPI e non di un mero atto interno della singola Istituzione Scolastica, scaturita dalla diversa efficacia delle singole fonti; solo il primo, infatti, in quanto fonte normativa, è suscettibile di incidere su diritti e libertà fondamentali di terzi.
VISTA la necessità di dare adeguata pubblicità, e un espresso riferimento nell'informativa da rendere agli interessati (art. 22, comma 2, del Codice).
DISPONE L'adozione del Regolamento il Decreto del Ministero della Pubblica Istruzione n. 305 del 7 dicembre 2006 (Regolamento) integrato con note - - da parte dell'Istituto con la necessità di rivedere e modificare alcuni atti già adottati e i procedimenti interni alla scuola seguiti nel trattamento dei dati sensibili e giudiziari.
Operando affinchè:

nel Documento Programmatico per la Sicurezza la parte relativa all'elenco dei dati personali trattati (punto 19.1 del Disciplinare tecnico, All. B – D. Lgs. 196/2003) sia adeguata alle prescrizioni e indicazioni contenute nelle schede;
il Titolare del trattamento (Dirigente Scolastico) adegui la nomina del Responsabile del trattamento richiamando le prescrizioni contenute nel Regolamento e fornendo gli indirizzi per la loro attuazione nei procedimenti amministrativi e nella gestione delle attività;
il Responsabile del trattamento (per la parte relativa al personale posto alle sue dirette dipendenze) e il Titolare del trattamento (per il personale docente) adeguino le designazioni degli incaricati del trattamento (cd lettere d'incarico), modificando, se necessario, le autorizzazioni concesse e le linee guida emanate;
la conoscenza del Regolamento sia oggetto dell'attività di formazione del personale incaricato prevista dal D.L.vo 196/03;
nell'informativa agli interessati si faccia riferimento al rispetto da parte della scuola alle prescrizione del Regolamento;
sia data evidenza dell'aggiornamento del Documento Programmatico sulla Sicurezza (All. B Regola 19
D. Lgs. 196/2003) effettuato entro il 30 marzo 2007

LINEE GUIDA IN MATERIA DI SICUREZZA PER

IL DOCENTE
INCARICATO DEL TRATTAMENTO

Vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:

- Custodire in apposito armadio dotato di serratura nella stanza individuata come sala professori dell'edificio i seguenti documenti:

1. Registro personale
2. Certificati medici esibiti dagli alunni a giustificazione delle assenze
3. Qualunque altro documento contenente dati personali o sensibili degli alunni

Verificare la corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al responsabile di sede eventuali anomalie.

- Consegnare il registro di classe al collaboratore scolastico incaricato, al termine delle attività didattiche giornaliere, per la sua custodia in apposito armadio dotato di serratura nella stanza individuata come sala professori dell'edificio.

- Seguire le istruzioni del docente responsabile dell'aula di informatica.

- Seguire le istruzioni del docente responsabile di sede nel caso di trattamento dei dati personali per fini diversi da quelli relativi ai punti 1 e 2.

- Tutte le comunicazioni indirizzate agli uffici della sede centrale, ad altro personale della scuola e al dirigente scolastico debbono essere consegnate in busta chiusa al responsabile di sede o al protocollo della sede centrale. Non è consentito, se non espressamente autorizzato, l'utilizzo del fax, della posta elettronica e dei collegamenti alla rete internet per il trattamento dei dati personali.

Per i docenti che utilizzano l'aula di informatica (nel caso di trattamento di dati personali) e per il responsabile dell'aula di informatica:

Seguire le seguenti istruzioni operative per l'utilizzo dei personal computers:

- Non lasciare floppy disk, cartelle o altri documenti a disposizione di estranei;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
    1. originale
    2. composta da otto caratteri
    3. che contenga almeno un numero
    4. che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
- curare la conservazione della propria password ed evitare di comunicarla ad altri;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
- trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del computer;
- utilizzare le seguenti regole per la posta elettronica:
    1. non aprire documenti di cui non sia certa la provenienza
    2. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
    3. controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali

IL DIRIGENTE SCOLASTICO

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL COLLABORATORE SCOLASTICO INCARICATO DEL TRATTAMENTO

Vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali:

(collaboratore scolastico in servizio nelle sedi ed ai piani)
Accertarsi che al termine delle lezioni non restino incustoditi i seguenti documenti, segnalandone tempestivamente l'eventuale presenza al responsabile di sede e provvedendo temporaneamente alla loro custodia:

- Registro personale dei docenti
- Registro di classe
- Certificati medici esibiti dagli alunni a giustificazione delle assenze
- Qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti

Accertarsi che al termine delle lezioni tutti i computers dell'aula di informatica siano spenti e che non siano stati lasciati incustoditi floppy disk, cartelle o altri materiali, in caso contrario segnalarne tempestivamente la presenza al responsabile di laboratorio o di sede e provvedendo temporaneamente alla loro custodia.

Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.

Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.

(collaboratore scolastico in servizio negli uffici di segreteria)
Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati.

Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte.
Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e non annotarne il contenuto sui fogli di lavoro.
Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati.
Non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o sensibili.
Segnalare tempestivamente al Responsabile del trattamento la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia.
Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale.
Procedere alla chiusura dei locali di segreteria accertandosi che siano state attivate tutte le misure di protezione e che le chiavi delle stanze siano depositate negli appositi contenitori.
Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si stati espressamente autorizzati dal Responsabile o dal Titolare.

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

Responsabile del trattamento dati

LINEE GUIDA IN MATERIA DI SICUREZZA PER L' ASSISTENTE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO

Attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari :

- Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato, dotato di serratura;
- Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Responsabile eventuali anomalie;
- Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
- Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
- Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
- Non consentire l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;
- Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
- Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;

- Segnalare tempestivamente al Responsabile la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
- Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Responsabile o dal Titolare.

Riguardo ai trattamenti eseguiti con supporto informatico attenersi scrupolosamente alle seguenti indicazioni:

- Non lasciare floppy disk, cartelle o altri documenti a disposizione di estranei;
- Conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
  - originale
  - composta da otto caratteri
  - che contenga almeno un numero
  - che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
- curare la conservazione della propria password ed evitare di comunicarla ad altri;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
- trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del computer;

- non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
- non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
- utilizzare le seguenti regole per la posta elettronica:
  - non aprire documenti di cui non sia certa la provenienza
  - non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
  - inviare messaggi di posta solo se espressamente autorizzati dal Responsabile
  - controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

Responsabile del trattamento dati

Lettera di nomina dell'incaricato del trattamento dei dati personali

All'Ins.

_____

IL DIRIGENTE SCOLASTICO

In qualità di Titolare del trattamento dei dati personali dell'Istituzione scolastica;
Ai sensi degli art. 29 e 30 del Testo Unico in materia di trattamento dei dati personali D.lgs 196/03;
Tenuto conto della funzione svolta dalla S.V. nell'istituzione scolastica ai sensi degli articoli dal 22 al 34 del CCNL vigente del Comparto scuola ;

Considerato che, nell'ambito di tale funzione, la S.V. compie operazioni di trattamento dei dati personali nel rispetto delle norme previste in materia;
Visto il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione emanato con Decreto Ministeriale n.305 del 7.12.2006;
Visto il Documento Programmatico della Sicurezza adottato dall'istituzione scolastica;

NOMINA la S.V.
INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

La S.V. è pertanto autorizzata, nell'espletamento delle attività connesse alla funzione docente, all'accesso e al trattamento dei dati personali di alunni e genitori, nella misura e nei limiti dal Testo Unico e dal Regolamento citati nelle premesse.

Istruzioni specifiche sul trattamento dei dati personali
Nello svolgimento dell'incarico la S.V. avrà accesso ai dati personali gestiti da questa istituzione scolastica e dovrà attenersi alle seguenti istruzioni, ai sensi dell'art. 11 del D.lgs 196/2003:

- Trattare i dati personali in modo lecito e secondo correttezza;

- Raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- Fornire sempre l'informativa agli interessati, ai sensi dell'art 13 del D.lgs 196/2003, utilizzando i moduli appositamente predisposti;
- Informare prontamente il Titolare e il Responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
- Informare prontamente il Titolare e il Responsabile del trattamento qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alla S.V.;
- Accedere solo ai dati strettamente necessari all'esercizio delle proprie funzioni;
- Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare;

- Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
- Relazionarsi e collaborare con gli altri incaricati del trattamento dei dati, attenendosi alle indicazioni fornite e provvedendo, a propria volta, a dare indicazioni esaustive in caso di coinvolgimento di altri incaricati nei trattamenti effettuati;
- Rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, indicate nel Documento Programmatico della Sicurezza dell'istituto e nelle allegate "Linee guida" elaborate ai sensi dell'art. 31 del D.Lvo 196/2003;
- Seguire le attività di formazione organizzate dalla istituzione scolastica per gli incaricati del trattamento dati;
- Partecipare alla attività di verifica e revisione del Documento Programmatico della Sicurezza.

Istruzioni specifiche sul trattamento dei dati sensibili e giudiziari

Relativamente ai dati sensibili e giudiziari forniti dagli alunni e dalle famiglie e nell'espletamento delle attività connesse alla funzione docente, la S.V. effettuerà i trattamenti consentiti indicati nelle schede, allegate al Regolamento, n. 4 (attività propedeutiche all'inizio dell'anno scolastico),n. 5 (attività educativa, didattica e formativa, di valutazione) e n.7 (rapporti scuola famiglie: gestione del contenzioso) per le finalità di rilevante interesse pubblico indicate e limitatamente ai tipi di dati trattati ed alle operazioni che sono precisate sia come particolari forme di trattamento che come altre tipologie più ricorrenti di trattamento.

La presente nomina di Incaricato al trattamento dei dati personali è a tempo indeterminato e può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati personali senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità, ai sensi delle norme contenute nel D.lgs 196/03.

IL DIRIGENTE SCOLASTICO

Titolare del trattamento dati

Il sottoscritto ……. dichiara di aver ricevuto la presente nomina ad Incaricato del trattamento dei dati personali, corredata dalle "Linee Guida in materia di sicurezza" e dalle schede n.4, n.5 e n.7, allegate al Regolamento di identificazione dei dati sensibili e giudiziari e delle relative operazioni effettuate, e si impegna a seguirne e rispettarne tutte le specifiche istruzioni, attentamente esaminate e comprese. Il sottoscritto si impegna altresì a prendere visione e conoscere il Documento Programmatico della Sicurezza, seguendone i periodici aggiornamenti, e a rispettare il divieto di comunicazione e diffusione dei dati trattati nel corso del presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

…… …….

(data) (firma dell'incaricato

Lettera di nomina dell'incaricato del trattamento dei dati personali

Al collaboratore scolastico

_____

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

In qualità di Responsabile del trattamento dei dati personali dell'Istituzione scolastica;
Ai sensi degli art. 29 e 30 del Codice in materia di protezione dei dati personali D.Lgs 196/03;

Tenuto conto del ruolo funzionale svolto dalla S.V. nell'istituzione scolastica ai sensi della Tabella A, area A del vigente CCNL del Comparto scuola;
Considerato che, nell'ambito di tali mansioni, la S.V. compie attività che possono comprendere il trattamento dei dati personali;
Visto il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione emanato con Decreto Ministeriale n.305 del 7.12.2006;
Visto il Documento Programmatico della Sicurezza adottato dall'istituzione scolastica;

NOMINA la S.V.
INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

La S.V. è pertanto autorizzata all'accesso e al trattamento dei dati personali in occasione della gestione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta e del trasferimento fra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali e dati sensibili e giudiziari nei limiti dei trattamenti consentiti dal Regolamento citato in premessa.

Istruzioni specifiche sul trattamento dei dati
Nello svolgimento dell'incarico la S.V. avrà accesso ai dati personali gestiti da questa istituzione scolastica e dovrà attenersi alle seguenti istruzioni, ai sensi dell'art. 11 del D.Lgs 196/2003:
- Trattare i dati personali in modo lecito e secondo correttezza;

- Raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale
- Informare prontamente il Titolare e il Responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
- Informare prontamente il Titolare e il Responsabile del trattamento qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alla S.V.
- Accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile;
- Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della sua identità;
- Relazionarsi e collaborare con gli altri incaricati del trattamento dei dati, attenendosi alle indicazioni fornite e provvedendo, a propria volta, a dare indicazioni esaustive in caso di coinvolgimento di altri incaricati nei trattamenti effettuati;
- Seguire le attività di formazione organizzate dalla istituzione scolastica per gli incaricati del trattamento dati;

- Partecipare alla attività di verifica e revisione del documento programmatico della sicurezza.

Istruzioni specifiche sul trattamento dei dati sensibili e giudiziari

La S.V., relativamente ai dati sensibili e giudiziari, nel caso in cui sia coinvolta nel loro trattamento, si atterrà alle specifiche istruzioni impartite dal titolare, dal responsabile e dagli incaricati dei trattamenti stessi.

La presente nomina di Incaricato al trattamento dei dati personali è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità, ai sensi delle norme contenute nel D.Lgs 196/03.

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

Responsabile del trattamento dati

_____

Il sottoscritto ……. dichiara di aver ricevuto la presente nomina ad Incaricato del trattamento dei dati personali, corredata dalle "Linee Guida in materia di sicurezza" e si impegna a seguirne e rispettarne tutte le specifiche istruzioni, attentamente esaminate e comprese. Il sottoscritto si impegna altresì a rispettare il divieto di comunicazione e diffusione dei dati trattati nel corso del presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

……. …….

(data) (firma dell'incaricato

Lettera di nomina dell'incaricato del trattamento dei dati personali

All'assistente amministrativo

_____

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

In qualità di Responsabile del trattamento dei dati personali dell'Istituzione scolastica;
Ai sensi degli art. 29 e 30 del Codice in materia di protezione dei dati personali D.lgs 196/03;

Tenuto conto del ruolo funzionale svolto dalla S.V. nell'istituzione scolastica ai sensi della Tabella A, area B del vigente CCNL del Comparto scuola;
Considerato che, nell'ambito di tale funzione, la S.V. compie operazioni di trattamento dei dati personali nel rispetto delle norme previste in materia;
Visto il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione emanato con Decreto Ministeriale n.305 del 7.12.2006;

NOMINA la S.V.

INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

La S.V. è pertanto autorizzata all'accesso e al trattamento dei dati personali di tutti i soggetti con i quali l'istituzione scolastica entra in relazione per i suoi fini istituzionali, nella misura e nei limiti previsti dalle mansioni assegnate, dagli ordini di servizio ricevuti e dalle istruzioni ivi contenute e nel rispetto del Testo Unico e del Regolamento citati nelle premesse.

In particolare, alla S.V. è affidato l'incarico di trattare i dati personali relativi all'area di assegnazione risultante dal piano delle attività e dagli ordini di servizio.

Istruzioni specifiche sul trattamento dei dati personali

Nello svolgimento dell'incarico la S.V. avrà accesso alle banche dati gestite da questa istituzione scolastica e dovrà attenersi alle seguenti istruzioni, ai sensi dell'art. 11 del D.Lgs 196/2003:

- Trattare i dati personali in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;
- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- Comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- Non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- Fornire sempre l'informativa agli interessati, ai sensi dell'art 13 del D.lvo 196/2003, utilizzando i moduli appositamente predisposti;
- Accertarsi che gli interessati abbiano autorizzato l'uso dei dati richiesti;
- Informare prontamente il Titolare e il Responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
- Informare prontamente il Titolare e il Responsabile del trattamento qualora verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite alla S.V.;

- Accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- Accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile;
- Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
- Relazionarsi e collaborare con gli altri incaricati del trattamento dei dati, attenendosi alle indicazioni fornite e provvedendo, a propria volta, a dare indicazioni esaustive in caso di coinvolgimento di altri incaricati nei trattamenti effettuati;
- Rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati, indicate nelle allegate "Linee guida in materia di sicurezza" elaborate ai sensi dell'art. 31 del D.lgs 196/2003;
- Seguire le attività di formazione organizzate dalla istituzione scolastica per gli incaricati del trattamento dati;
- Partecipare alla attività di verifica e revisione del documento programmatico della sicurezza.

Istruzioni specifiche sul trattamento dei dati sensibili e giudiziari
Relativamente ai dati sensibili e giudiziari di tutti i soggetti con i quali l'istituzione scolastica entra in relazione per i suoi fini istituzionali, la S.V. effettuerà, qualora assegnato a settori di lavoro che li richiedano, i trattamenti consentiti indicati nelle schede, allegate al Regolamento, n.1 (Selezione e reclutamento a tempo indeterminato e determinato e gestione del rapporto di lavoro), n.3 (Organismi collegiali e commissioni istituzionali) n. 4 (attività propedeutiche all'inizio dell'anno scolastico) e n. 5 (attività educativa, didattica e formativa, di valutazione), per le finalità di rilevante interesse pubblico indicate e limitatamente ai tipi di dati trattati ed alle operazioni che sono precisate sia come particolari forme di trattamento che come altre tipologie più ricorrenti di trattamento.

La presente nomina di incaricato al trattamento dei dati personali è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S.V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.
Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità, ai sensi delle norme contenute nel D.lgs 196/03.

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

Responsabile del trattamento dati

_____

Il sottoscritto …… dichiara di aver ricevuto la presente nomina ad Incaricato del trattamento dei dati personali, corredata dalle "Linee Guida in materia di sicurezza" e dalle schede n.1, n.3, n.4 e n.5, allegate al Regolamento di identificazione dei dati sensibili e giudiziari e delle relative operazioni effettuate, e si impegna a seguirne e rispettarne tutte le specifiche istruzioni, attentamente esaminate e comprese. Il sottoscritto si impegna altresì a rispettare il divieto di comunicazione e diffusione dei dati trattati nel corso del presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

……
……
(data) (firma dell'incaricato)

Oggetto: Decreto legislativo 196/2003 "Codice in materia di protezione dei dati personali". Informativa all'interessato.

Secondo quanto previsto dall'art. 13 del D.lgs 196/2003 "Codice in materia di protezione dei dati personali" recante disposizioni sulla tutela della persona e di altri soggetti rispetto al trattamento di dati personali, questa Istituzione Scolastica, rappresentata dal dirigente scolastico prof._____ in qualità di Titolare del trattamento dei dati personali, per espletare le sue funzioni istituzionali e in particolare per gestire il rapporto di lavoro (per il personale con contratto a tempo indeterminato) da Lei instaurato con il MPI o (per il personale con contratto a tempo determinato e per i collaboratori esterni alla scuola e soggetti che intrattengono rapporti di lavoro diversi da quello subordinato) da Lei instaurato con la scuola, deve acquisire o già detiene dati personali che La riguardano, inclusi quei dati che il D.lgs 196/2003 definisce "dati sensibili e giudiziari".
Ai sensi del Decreto del Ministero della Pubblica Istruzione n. 305 del 7 dicembre 2006, che ha individuato i dati sensibili e giudiziari che le amministrazioni scolastiche sono autorizzate a trattare, indicando anche le operazioni ordinarie che i diversi titolari devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico individuate per legge, Vi informiamo che, per le esigenze di gestione sopra indicate, possono essere oggetto di trattamento le seguenti categorie di dati sensibili e giudiziari:

a) Relativamente alle operazioni di selezioni di reclutamento indeterminato e determinato e alla gestione del rapporto di lavoro anche diverso da quello subordinato:

- dati inerenti lo stato di salute trattati per l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c. d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sui luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative, pensionistiche e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o

sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;

- dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;
- dati sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione;
- dati sulle convinzioni filosofiche o d'altro genere che possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;
- dati di carattere giudiziario trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato;
- informazioni sulla vita sessuale che possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso;

b) Relativamente alla gestione del contenzioso e dei procedimenti disciplinari:

- dati sensibili e giudiziari concernenti tutte le attività relative alla difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

c) Relativamente al funzionamento degli Organismi collegiali e delle commissioni istituzionali:

- dati sensibili (appartenenza alle organizzazioni sindacali) necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'ordinamento scolastico.

d) Relativamente alla gestione del contenzioso tra la scuola e le famiglie degli alunni:

- dati sensibili e giudiziari concernenti tutte le attività connesse alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.

La informiamo inoltre che il trattamento dei suoi dati personali avrà le seguenti finalità:

- elaborazione, liquidazione e corresponsione della retribuzione, degli emolumenti, dei compensi dovuti e relativa contabilizzazione;
- adempimento di obblighi derivanti da leggi, contratti, regolamenti in materia di previdenza e assistenza anche integrativa e complementare, di igiene e sicurezza del lavoro, in materia fiscale, in materia assicurativa;
- tutela dei diritti in sede giudiziaria.

Le forniamo a tal fine le seguenti ulteriori informazioni:

- Il trattamento dei Suoi dati personali sarà improntato a principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti;
- I Suoi dati personali verranno trattati anche con l'ausilio di strumenti elettronici o comunque automatizzati con le modalità e le cautele previste dal predetto Decreto e conservati per il tempo necessario all'espletamento delle attività istituzionali e amministrative riferibili alle predette finalità;

- Sono adottate dalla scuola le misure minime per la sicurezza dei dati personali previste dal Decreto;
- Il titolare del trattamento è il dirigente scolastico prof._____;
- Il responsabile del trattamento è il Direttore dei Servizi Generali e Amministrativi sig.r_____;
- Gli incaricati al trattamento sono gli assistenti amministrativi espressamente autorizzati all'assolvimento di tali compiti, identificati ai sensi di legge, ed edotti dei vincoli imposti dal D.lgs n. 196/2003;
- I dati oggetto di trattamento potranno essere comunicati ai seguenti soggetti esterni all'istituzione scolastica per fini funzionali:
  - Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 145/2000;
  - Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
  - Organi preposti al riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001;
  - Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (D.lgs. n. 626/1994)
  - Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del D.P.R. n. 1124/1965;
  - Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68/1999;
  - Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
  - Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
  - Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 186;
  - Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e D.P.R. 20 febbraio 1998, n.38;
  - Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;

- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335;
- Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, D.lgs. n. 165/200 1).
- Alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
- Alle Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;
- Ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.

Le ricordiamo infine:

- che il conferimento dei dati richiesti è indispensabile a questa istituzione scolastica per l'assolvimento dei suoi obblighi istituzionali e il consenso non è richiesto per i soggetti pubblici e quando il trattamento è previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- che, ai sensi dell'art. 24 del D.lgs 196/2003, in alcuni casi il trattamento può essere effettuato anche senza il consenso dell'interessato;
- che in ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art. 7 del D.lgs 196/2003 .

In allegato alla presente informativa sono riportati gli articoli 7 e 24 del D.lgs 196/2003

IL DIRIGENTE SCOLASTICO

Titolare del trattamento dati

Al genitori dell'alunna/o _____

Oggetto: D.lgs 196/2003 "Codice in materia di protezione dei dati personali". Informativa all'interessato.

Secondo quanto previsto dall'art. 13 del D.lgs 196/2003 "Codice in materia di protezione dei dati personali" recante disposizioni sulla tutela della persona e di altri soggetti, rispetto al trattamento di dati personali, questa Istituzione Scolastica, rappresentata dal dirigente scolastico prof._____, in qualità di Titolare del trattamento dei dati personali, per espletare le sue funzioni istituzionali e, in particolare, per gestire le attività di istruzione, educative e formative stabilite dal Piano dell'Offerta Formativa, deve acquisire o già detiene dati personali che Vi riguardano, inclusi quei dati che il D.lgs 196/2003 definisce "dati sensibili e giudiziari".
Ai sensi del Decreto del Ministero della Pubblica Istruzione n. 305 del 7 dicembre 2006 che ha individuato i dati sensibili e giudiziari che le amministrazioni scolastiche sono autorizzate a trattare, indicando anche le operazioni ordinarie che i diversi titolari devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico individuate per legge, Vi informiamo che, per le esigenze di gestione sopra indicate, possono essere oggetto di trattamento le seguenti categorie di dati sensibili e giudiziari:
a) nelle attività propedeutiche all'avvio dell'anno scolastico:

- dati relativi alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana;
- dati relativi alle convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- dati relativi allo stato di salute, per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi;
- dati relativi alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione (i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti degli alunni che abbiano commesso reati).

b) nell'espletamento dell'attività educativa, didattica, formativa e di valutazione:

- dati relativi alle origini razziali ed etniche per favorire l'integrazione degli alunni con cittadinanza non italiana;
- dati relativi alle convinzioni religiose per garantire la libertà di credo religioso;
  dati relativi allo stato di salute, per assicurare 1 'erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;
- dati giudiziari, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
- dati relativi alle convinzioni politiche, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori.

c) nella gestione del contenzioso tra la scuola e le famiglie degli alunni:

- dati sensibili e giudiziari concernenti tutte le attività connesse alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali

Vi informiamo inoltre che il trattamento dei vostri dati personali avrà le seguenti finalità:

- partecipazione degli alunni alle attività organizzate in attuazione del Piano dell'Offerta Formativa;
- adempimento di obblighi derivanti da leggi, contratti, regolamenti in materia di igiene e sicurezza del lavoro, in materia fiscale, in materia assicurativa;
- tutela dei diritti in sede giudiziaria.

Vi forniamo a tal fine le seguenti ulteriori informazioni:

- Il trattamento dei dati personali sarà improntato a principi di correttezza, liceità e trasparenza e di tutela della Vostra riservatezza e dei Vostri diritti anche in applicazione dell'art.2 del DPR n.249/1998;
- I dati personali verranno trattati anche con l'ausilio di strumenti elettronici o comunque automatizzati con le modalità e le cautele previste dal predetto D.lgs e conservati per il tempo necessario all'espletamento delle attività istituzionali e amministrative riferibili alle predette finalità;
- Sono adottate dalla scuola le misure minime per la sicurezza dei dati personali previste dal D.lgs;
- Il titolare del trattamento è il dirigente scolastico prof.re _____;
- Il responsabile del trattamento è il Direttore dei Servizi Generali e Amministrativi Sig.r_____;
- Gli incaricati al trattamento dati sono gli assistenti amministrativi sig.r_____, espressamente autorizzati all'assolvimento di tali compiti, identificati ai sensi di legge, ed edotti dei vincoli imposti dal D.lgs;
- I dati oggetto di trattamento potranno essere comunicati ai seguenti soggetti esterni all'istituzione scolastica per le seguenti finalità:
  - Alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
  - Agli Enti Locali per la fornitura dei servizi ai sensi del D.Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
  - Ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
  - Agli Istituti di assicurazione per denuncia infortuni e per la connessa responsabilità civile;
  - All'INAIL per la denuncia infortuni ex D.P.R. 30 giugno 1965, n. 1124;

- Alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della legge 5 febbraio 1992, n.104;
- Ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D.Lgs 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio;
- Alle Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
- Alle Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;
- Ai liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.

Vi ricordiamo infine:

- che il conferimento dei dati richiesti è indispensabile a questa istituzione scolastica per l'assolvimento dei suoi obblighi istituzionali;
- che, ai sensi dell'art. 24 del D.lgs 196/2003, in alcuni casi il trattamento può essere effettuato anche senza il consenso dell'interessato;
- che in ogni momento potrete esercitare i vostri diritti nei confronti del titolare del trattamento, ai sensi dell'art. 7 del D.lgs 196/2003;
- che potrete richiedere di avvalervi della possibilità prevista dall'art.96 D.lgs 196/2003 di comunicazione e diffusione dei dati personali necessari ad agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero e per via telematica.

In allegato alla presente informativa sono riportati gli articoli 7, 24, 73 e 96 del D.lgs 196/2003 e l'art.2 del DPR 249/1998.

IL DIRIGENTE SCOLASTICO

Titolare del trattamento dati

Al responsabile della ditta _____

Oggetto: Decreto legislativo 196/2003 "Codice in materia di protezione dei dati personali". Informativa all'interessato.

Secondo quanto previsto dall'art. 13 del D. LGS 196/2003 "Codice in materia di protezione dei dati personali" recante disposizioni sulla tutela della persona e di altri soggetti rispetto al trattamento di dati personali, questa Istituzione Scolastica, rappresentata dal dirigente scolastico prof. r_____in qualità di Titolare del trattamento dei dati personali, per espletare le sue funzioni istituzionali e in particolare per gestire i rapporti contrattuali instaurati o da instaurare deve acquisire o già detiene dati personali che La riguardano.
La informiamo inoltre che il trattamento dei suoi dati personali avrà le seguenti finalità:

- predisposizione comunicazioni informative precontrattuali e istruttorie rispetto alla stipula di un contratto;
- esecuzione del contratto e sua gestione amministrativa: elaborazione, liquidazione e corresponsione degli importi dovuti e relativa contabilizzazione;
- analisi del mercato e elaborazioni statistiche;
- verifica del grado di soddisfazione dei rapporti;
- adempimento di obblighi derivanti da leggi, contratti, regolamenti in materia di igiene e sicurezza del lavoro, in materia fiscale, in materia assicurativa;
- tutela dei diritti in sede giudiziaria.

Le forniamo a tal fine le seguenti ulteriori informazioni:

- Il trattamento dei Suoi dati personali sarà improntato a principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti;
- I dati personali trattati sono esclusivamente quelli necessari e pertinenti alle finalità del trattamento;
- I Suoi dati personali verranno trattati anche con l'ausilio di strumenti elettronici o comunque automatizzati con le modalità e le cautele previste dal D.Lgs. n. 196/2003 e conservati per il tempo necessario all'espletamento delle

attività istituzionali, gestionali e amministrative riferibili alle predette finalità;

- Il titolare del trattamento è il dirigente scolastico Prof.r_____;
- Il responsabile del trattamento è il Direttore dei Servizi Generali e Amministrativi Sig.r_____;
- Gli incaricati al trattamento sono il prof.re _____, responsabile dell'Ufficio Tecnico e l'assistente amministrativo sig.r_____, espressamente autorizzati all'assolvimento di tali compiti, identificati ai sensi di legge, ed edotti dei vincoli imposti dal D.Lgs. n. 196/2003;
- I dati oggetto di trattamento potranno essere comunicati ai seguenti soggetti esterni all'istituzione scolastica per fini connessi o funzionali al miglioramento dell'efficacia e dell'efficienza dei servizi amministrativi e gestionali: MPI, Ufficio Scolastico Regionale del _____, Ufficio Scolastico Provinciale di _____, Altre istituzioni scolastiche, Amministrazione Regionale del _____, Amministrazione Provinciale di _____, Comune di _____, Organizzazioni Sindacali, Agenzia delle Entrate, Banca che effettua il servizio di cassa, Organi preposti alla vigilanza su igiene e sicurezza, AUSL, Collegio Revisori dei Conti e persone fisiche e giuridiche responsabili di attività connesse con il funzionamento dell'istituzione scolastica.

Le ricordiamo infine:

- che il conferimento dei dati richiesti è indispensabile a questa istituzione scolastica per l'assolvimento dei suoi obblighi istituzionali e il consenso non è richiesto per i soggetti pubblici e quando il trattamento è previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- che il conferimento dei dati richiesti è indispensabile a questa istituzione scolastica per l'assolvimento dei suoi obblighi istituzionali e contrattuali, pertanto il mancato consenso al trattamento può comportare il mancato o parziale espletamento di tali obblighi;
- che in ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art. 7 del D. LGS 196/2003 riportato in calce alla presente comunicazione.

IL DIRIGENTE SCOLASTICO

Titolare del trattamento dati

D.P.S. 2007

Il Dirigente scolastico

Visto il decreto legislativo 30 giugno 2003, n.196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 33 e ss., nonché l'allegato B del suddetto D.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

Considerato che l' _____istituto scolastico_____ è titolare del trattamento di dati personali ai sensi dell'art.28 del d.lgs. n. 196 del 2003;
Visto l'obbligo di prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del D.lgs. n.196 del 2003;
Visto il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, emanato con Decreto Ministeriale n.305 del 7.12.2006;

Adotta il DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento, elaborato al fine di mettere in atto le misure di sicurezza per tutelare i dati personali oggetto di trattamento, fornisce una individuazione dei criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati a misure di sicurezza e dei criteri per assicurare l'integrità dei dati, da adottare per il trattamento dei dati personali effettuato dal personale dell' _____istituto scolastico_____ il cui legale rappresentante pro-tempore è il dirigente scolastico prof. _____ che nel seguito del documento sarà indicato come "titolare". Il presente documento è aggiornato periodicamente ed i termini utilizzati seguono le definizioni riportate all'art.4 del D.lgs 196/2003. Del documento fanno parte integrante le schede allegate al Regolamento del Ministero della Pubblica Istruzione citato nelle premesse.

1 Elenco dei trattamenti di dati personali

1.1 Finalità

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore, con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di rilevante interesse pubblico, ai sensi degli articoli 20 e 21 del D.lgs 196/2003.

Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni che sensibili o giudiziari, di studenti, genitori, personale dipendente e fornitori.

1.2 Luoghi di tenuta e trattamento dei dati:

I dati su supporto cartaceo sono conservati negli armadi degli uffici: amministrativo, del personale, didattica alunni, ufficio tecnico e nella stanza del protocollo, nella stanza denominata archivio corrente e nella stanza denominata archivio storico.
I dati acquisiti attraverso il protocollo riservato sono conservati nella cassaforte dell'ufficio del dirigente scolastico.
I dati su supporto elettronico sono conservati negli archivi elettronici dei computer di tutti i servizi amministrativi.

(Nella tabella che segue, relativamente ai dati sensibili e giudiziari, nella descrizione sintetica del trattamento, le finalità e le attività svolte, i tipi di dati trattati e le operazioni eseguite sono indicati in modo sintetico e con riferimento alle schede allegate al Regolamento del Ministero della Pubblica Istruzione citato nelle premesse, con specificazione, per ogni identificativo di trattamento, delle specifiche schede)

Tabella 1.1 – Elenco dei trattamenti: informazioni essenziali (regola 19.1 del disciplinare tecnico)

Id Trattamento	*Descrizione sintetica del trattamento*			*Na d*
	Finalità perseguita o attività svolta	***Categorie di interessati***	***Terzi a cui vengono comunicati i dati***	***S***
T1	**Gestione Area Alunni** Relativamente ai dati sensibili e giudiziari : Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico; Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	**Alunni Genitori**	**USP, MPI, Altre istituzioni scolastiche, AUSL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, Aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola lavoro, Avvocature dello Stato, Magistrature ordinarie e amministrativo-contabile, Organi di polizia giudiziaria, Liberi professionisti**	**S**
T2	**Gestione Area Bilancio**	**Personale Fornitori**	**USP, USR, MPI, Agenzia delle Entrate, Altre istituzioni scolastiche, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Banca che effettua il servizio di cassa**	
T3	**Gestione Area Personale** Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari; Scheda n. 3 – Organismi collegiali e commissioni istituzionali; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	**Personale**	**USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego**	**S**

T4	**Gestione Area Retribuzioni** Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari; Scheda n. 3 – Organismi collegiali e commissioni istituzionali;	**Personale**	**USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Magistrature ordinarie e amministrativo-contabile,Agenzia delle Entrate, Banca che effettua il servizio di cassa**	**S**
T5	**Gestione Fiscale**	**Personale**	**USP, MPI, Agenzia delle Entrate, Corte dei Conti, Enti assistenziali, previdenziali e assicurativi, MEF, Banca che effettua il servizio di cassa**	
T6	**Gestione Protocollo** Relativamente ai dati sensibili e giudiziari: Tutte le schede allegate al regolamento sul trattamento dei dati sensibili e giudiziari	**Alunni, Genitori, Fornitori, Personale, Altre amministrazioni**	**USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego, Banca che effettua il servizio di cassa**	**S**
T7	**Gestione Sicurezza**	**Personale amministrativo accesso aree Axios**		
T8	**Backup e Restore**	**Banca dati Amministrativa**		
T9	**Gestione Protocollo e corrispondenza riservata** Relativamente ai dati sensibili e giudiziari: Tutte le schede allegate al regolamento sul trattamento dei dati sensibili e giudiziari	**Alunni, genitori, personale**	**USP, MPI, Altre istituzioni scolastiche, AUSL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, Aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola lavoro, Avvocature dello Stato, Magistrature ordinarie e amministrativo-contabile, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Organi di polizia giudiziaria, Liberi professionisti**	**S**

T10	**Gestione della posta elettronica**	**Personale, utenti del servizio scolastico, fornitori**		
T11	**Gestione Scioperi del Personale dipendente** Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;	**Personale**	**https://websptnet.tesoro.it/SCIOPNET**	**S**
T12	**Gestione Anagrafe delle prestazioni**	**Personale interno ed esterno, Fornitori**	**www.anagrafeprestazioni.it**	
T13	**Invio documenti tramite Entratel e DM10**	**Personale esterno e della scuola**	**Sito entratel**	
T14	**Gestione Pre96**	**Personale**	**Ragioneria Provinciale del Tesoro**	
T15	**Gestione INPS**	**Personale**	**INPS**	**S**
T16	**Gestione con Suite Microsoft Office comunicazione**	**Personale interno ed esterno, Fornitori**		
T17	**Gestione Dispostivi dell'infrastruttura tecnologica**	**Personale interno ed esterno, Fornitori**		
T18	**Gestione Provvedimenti Disciplinari alunni** Relativamente ai dati sensibili e giudiziari : Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico; Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	**Genitori, Alunni, Personale**	**Genitori, USP**	**S**

T19	**Gestione Graduatorie e supplenze**	**Personale**	**USP, USR, MPI**	
T20	**Gestione del personale**	**Personale**		**S**
T21	**Gestione III^ Area e Contratti prestazione**	**Personale interno ed esterno Alunni**	**Enti Pubblici Territoriali, INAIL, Organizzazioni Sindacali, Ditte Esterne**	
T22	**Gestione Trattative sindacali** Relativamente ai dati sensibili e giudiziari : Scheda n. 3 – Organismi collegiali e commissioni istituzionali;	**Contrattazione sindacale**	**Componenti RSU Organizzazioni Sindacali**	**S**
T23	**Gestione Archivio cartaceo storico**	**Tutte le categorie**	**I dati non vengono comunicati a terzi (prima dell'eventuale comunicazione vengono trasferiti alle strutture interne autorizzate al trattamento)**	**S**
T24	**Gestione Assistenza e manutenzione hardware**	**Tutti i soggetti che utilizzano i PC degli uffici Amministrativi**		
T25	**Gestione titolario Generale**		**USP, USR, MPI**	
T26	**Gestione Riproduzione e notifica documenti**	**Personale, Alunni, Genitori Fornitori**		
T27	**Gestione Atti cartacei amministrativi**	**Personale, Alunni, Genitori Fornitori**		
T28	**Gestione Inventario e Fornitori di beni e servizi**	**Ditte esterne**	**Ditte esterne**	

Tabella 1.2 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti (regola 19.1 del disciplinare tecnico)

Id Trattamento	**Applicativo**	*Banca Dati*	*Ubicazione fisica dei supporti di memorizzazione*	*Tipologia dei dispositivi*	*Tipologia di interconnessione*

			Luogo	*Elaboratore*	*di accesso*	
T1	**Software gestionale Axios**	**Serversissi**	**Salaserver**	**PC serversissi**	**PC**	**Internet - Intranet**
T2	**Software gestionale Axios**	**Serversissi**	**Salaserver**	**PC serversissi**	**PC**	**Internet - Intranet**
T3	**Software gestionale Axios**	**Serversissi**	**Salaserver**	**PC serversissi**	**PC**	**Internet - Intranet**
T4	**Software gestionale Axios**	**Serversissi**	**Salaserver**	**PC serversissi**	**PC**	**Internet - Intranet**
T5	**Software gestionale Axios**	**Serversissi**	**Salaserver**	**PC serversissi**	**PC**	**Internet - Intranet**
T6	**Software gestionale Axios**	**Serversissi**	**Salaserver**	**PC serversissi**	**PC**	**Internet - Intranet**
T7	**Software gestionale Axios**	**Serversissi**	**Salaserver**	**PC serversissi**	**PC**	**Internet - Intranet**
T8	**Software gestionale Axios**	**Serversissi**	**Salaserver**	**PC serversissi**	**PC**	**Internet - Intranet**
T9	**Suite Microsoft Office**	**PC Dirigente scolastico**	**Stanza Dirigente Scolastico**	**PC Dirigente**	**PC**	**Intranet**
T10	**Outlook Express – Area Riservata Ministero Istruzione**	**Pc Ufficio Personale**	**Ufficio Personale**	**Pc Uff. Personale**	**PC**	**Intranet**
T11	**Accesso area riservata Min. Tesoro**	**Ministero Tesoro**				
T12	**Sito Anagrafe delle Prestazioni**	**Ministero Istruzione**				
T13	**Sito riservato Agenzia Entrate**	**Agenzia Entrate**				

T14	**Software Ministero Tesoro**	**Agenzia entrate**				
T15						
T16	**Suite Microsoft Office**	**Pc Ufficio**	**Tutti gli uffici**	**Tutti gli Uffici**	**PC**	**Intranet**
T17						
T18	**Suite Microsoft Office**	**Pc Ufficio collaboratore Dirigente Scolastico**				
T19	**Accesso Area Riservata Ministero Istruzione**	**PC Ufficio Personale**	**PC Ufficio Personale**	**PC Ufficio Personale**		**Intranet**
T20	**Applicativo Axios**	**Serversissi**	**Serversissi**	**Serversissi**		**Intranet**
T21	**Suite Microsoft Office**	**Pc Ufficio**	**Pc Ufficio Protocollo**	**Pc Ufficio Protocollo**		**Intranet**
T22	**Suite Microsoft Office Archivio cartaceo**	**PC Dirigente scolastico**	**PC Dirigente scolastico**	**PC Dirigente Scolastico**		**Intranet**
T23	**Contenitori per archivio**	**Archivio storico**	**Archivio storico**	**Archivio storico**		
T24						
T25						
T26						
T27						
T28						

Tabella 1.3 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti cartacei (regola 19.1 del disciplinare tecnico)

Id Trattamento	***Archivio cartaceo***	***Ubicazione logistica***		
			Stanza	***Armadio***
T23	**Raccoglitori cartacei**	**Scaffalatura con raccoglitori specifici e numerati dell'ufficio**	**Archivio storico**	

T27	**Armadi e scaffali metallici**	**Scaffalatura con raccoglitori specifici e numerati dell'ufficio**	**Ufficio di competenza**	

2 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

Le misure indicate nel presente documento sono relative alla sede centrale dell'istituzione scolastica.

Le procedure di trattamento dei dati avvengono nella sola sede centrale, considerato che i dati oggetto delle misure indicate nel presente documento sono trattenuti presso le altri sedi solo per il tempo necessario a provvedere all'inoltro alla sede centrale. I dati sono trattenuti sotto la responsabilità degli incaricati (docenti e responsabile della sede) in cassetto chiuso del quale detengono la chiave. L'inoltro avviene in busta chiusa per il tramite del personale della scuola con consegna all'ufficio protocollo.

Il titolare del trattamento ha designato, ai sensi dell'art.29 D.lgs 196/2003, con atto scritto contenente analitiche istruzioni relative ai compiti affidati, il responsabile del trattamento nella persona del DSGA sig.._____

Il responsabile del trattamento ha provveduto, sulla base della lettera di designazione e delle disposizione dell'art.30, ad individuare gli incaricati del trattamento dei dati personali appartenenti ai profili professionali del personale ATA; ha conferito agli stessi l'incarico con atto scritto contenente puntuali istruzioni relative agli ambiti di trattamento consentiti, corredato da linee guida e con allegate le schede relative al trattamento dei dati sensibili e giudiziari.

Il Responsabile del trattamento ha provveduto altresì a individuare, nominare e incaricare per iscritto un incaricato della gestione e della manutenzione degli strumenti elettronici, un incaricato della custodia delle copie delle credenziali e un incaricato delle copie di sicurezza delle banche dati ai quali sono state fornite puntuali istruzioni relative ai compiti da svolgere. Il titolare ha direttamente provveduto ad individuare e incaricare il personale docente con atto che fornisce le istruzioni necessarie. I singoli incaricati, che hanno rilasciato ricevuta della avvenuta consegna della lettera di incarico, sono stati informati che l'ambito dei trattamenti autorizzati è suscettibile di aggiornamento periodico e che sono tenuti ad attenersi al divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

La comunicazione dei soggetti previsti dal D.lgs 196/2003 è avvenuta attraverso la pubblicazione all'albo della scuola dell'organigramma della scuola e delle responsabilità.

A tutti gli incaricati del trattamento di dati mediante strumento elettronico sono state conferite credenziali di autenticazioni (art.34, comma 1, lett.b) mediante parola chiave, conformi alle caratteristiche indicate nell'allegato B. Agli incaricati sono state fornite puntuali indicazioni per la modifica della parola chiave ogni tre mesi.

Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti (regola 19.2)

Id Struttura	*Struttura*	*Trattamenti effettuati*	*Descrizione dei compiti e delle responsabilità*

A1.1	**Ufficio Personale**	**T3 – T10 – T11**	• **Uso applicativo Axios** • **Gestione dei documenti office automation** • **Accesso all'area riservata del sito Istruzione** • **Accesso al servizio di gestione degli scioperi** • **Consultazione e archiviazione dei fascicoli personali dei dipendenti** • **Gestione del software per la rilevazione delle presenze del personale** • **Gestione della posta elettronica**
A1.2	**Ufficio Contabilità**	**T2 – T13 – T14**	• **Uso applicativo Axios Area contabilità** • **Gestione dei documenti office automation** • **Accesso all'area riservata del sito Istruzione** • **Gestione della documentazione cartacea relativa al bilancio** • **Invio Documenti Entratel** • **Invio documenti PRE96** • **Invio DMA**
A1.3	**Ufficio Protocollo**	**T6**	• **Uso applicativo Axios Area protocollo** • **Gestione dei documenti office automation** • **Stampe registro protocollo** • **Smistamento e archiviazione corrispondenza**
A1.4	**Organizzazione 3° Area**	**T12 –T21**	• **Gestione dei documenti office automation** • **Contratti personale esterno Istituzione scolastica** • **Tenuta registri Corsi 3° Area**
A2.1	**Ufficio Tecnico**	**T28**	• **Gestione dei documenti office automation** • **Tenuta Inventario beni** • **Rapporti con i fornitori** • **Gare e acquisti di beni e servizi**
A2.2	**Ufficio Didattica Alunni**	**1**	• **Utilizzo del'applicativo Axios Area Alunni** • **Gestione dei documenti di office automation** • **Accesso all'area del sito** www.istruzione.it • **Accesso al servizio di denuncia infortuni del sito** www.nbabrokers.it • **Consultazione e archiviazione**

			dei fascicoli personali degli alunni
A3.1	**Ufficio Dirigente Scolastico**	**T22 -T9**	• **Gestione degli Organi collegiali** • **Gestione dell'offerta formativa** • **Gestione della sicurezza sul posto di lavoro legge 626** • **Gestione della protezione dei dati personali** • **Relazioni sindacali** • **Rapporti con gli enti** • **Gestione Protocollo Riservato**
A3.2	**Ufficio Direttore Servizi Generali e Amministrativi**	**T1-T2-T3-T4-T5-T6-T7**	• **Gestione del Bilancio** • **Utilizzo di tutti gli applicativi Axios** • **Utilizzo Applicativo gestione Sicurezza** • **Gestione rapporti con il personale** • **Organizzazione del Lavoro ATA** • **Concessione credenziali accesso area riservata Istruzione.it**
A3.3	**Ufficio Collaboratore del D.S.**	**T18**	• **Gestione Provvedimenti disciplinari alunni** • **Rilevazione assenze alunni della scuola**
A4	**Amministratore di Sistema**	**T8 - T17 – T24**	• **Amministra il Server di sistema Serversissi con il Dbase SISSI** • **Amministra i sistemi operativi dei clients in rete** • **Amministra e configura il router per l'accesso ad internet** • **Provvede agli aggiornamenti degli applicativi Axios e la loro installazione** • **Predispone l'automazione del backup dell'archivio SISSI con l'applicativo Axios** • **Installa sui client della rete amministrativa idoneo Antivirus** • **Installa su tutte le macchine idonei programmi antispywere** • **Utilizza l'applicativo Axios Gestione Sicurezza per la gestione degli accessi e dei profili**

A5	**Personale Docente**	**T1**	• **Trattamento dati degli alunni**
A6	**Archivio storico**	**T23 – T27**	• **Gestione e archiviazione Atti Amministrativi dell'Istituzione Scolastica**
A7	**Personale Ausiliario**	**T26**	• **Riproduzione mediante fotocopiatura dei documenti e notifica degli stessi**

3 Analisi dei rischi che incombono sui dati

La ricognizione e l'analisi dei rischi, che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuita, in grado di recare pregiudizio ai dati personali trattati, è stata riportata nelle tabelle che seguono nelle quali gli eventi sono stati suddivisi in tre categorie:

1)Comportamenti degli operatori.

Sottrazione di credenziali di autenticazione; carenza di consapevolezza, disattenzione o incuria; comportamenti sleali o fraudolenti; errori materiali.

2) Eventi relativi agli strumenti.

Danno arrecato da virus informatici o di programmi suscettibili di recare danno; spamming o tecniche di sabotaggio; malfunzionamento, indisponibilità o usura degli strumenti; accessi esterni non autorizzati; intercettazione di informazioni in rete.

3) Eventi relativi al contesto fisico-ambientale.
Accessi non autorizzati a locali ad accesso ristretto; eventi distruttivi naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc) nonché dolosi, accidentali o dovuti ad incuria; guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc); errori umani nella gestione della sicurezza fisica.

I suddetti rischi sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione, adottando la seguente scansione:

Alta - Bassa - Molto Elevata - Media - Medio-Alta - Medio-Bassa

La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone l'impatto sulla sicurezza. le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

Tabella 3 – Analisi dei rischi (regola 19.3 del disciplinare tecnico)

	Id Rischio	***Rischi***	***Si/No***	***Descrizione dell'impatto sulla sicurezza (gravità:alta/media/ bassa)***

Comportamento degli operatori	**R1**	**Sottrazione di credenziali di autenticazione.**	**Si**	**Alta**
	R2	**Carenza di consapevolezza, disattenzione o incuria.**	**Si**	**Media**
	R3	**Comportamenti sleali o fraudolenti.**	**Si**	**Bassa**
	R4	**Errore materiale.**	**Si**	**Media**
Eventi relativi agli strumenti	**R5**	**Azione di *virus* informatici o di programmi suscettibili di recare danno.**	**Si**	**Alta**
	R6	***Spamming* o tecniche di sabotaggio.**	**Si**	**Alta**
	R7	**Malfunzionamento, indisponibilità o degrado degli strumenti.**	**Si**	**Media**
	R8	**Accessi esterni non autorizzati.**	**Si**	**Media**
	R9	**Intercettazione di informazioni in rete.**	**Si**	**Media**
Eventi relativi al contesto	**R10**	**Accessi non autorizzati a locali/reparti ad accesso ristretto.**	**Si**	**Bassa**
	R11	**Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc,) nonché dolosi, accidentali o dovuti ad incuria.**	**Si**	**Media**
	R12	**Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.).**	**Si**	**Media**
	R13	**Errori umani nella gestione della sicurezza fisica.**	**Si**	**Media**

4 Misure da adottare per garantire l'integrità e la disponibilità dei dati, non che la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

Contro i rischi d'intrusione i locali della sede centrale, unica sede nella quale sono detenuti dati soggetti a protezione, sono dotati di impianto d'allarme a sensori infrarossi, attivabile mediante digitazione d'un codice consegnato al personale dipendente. E' stata disposta l'attivazione dell'allarme al termine dell'orario di lavoro.

Per garantire la sicurezza delle aree in cui i dati sono trattati elettronicamente, sono state introdotte sui personal computer password di BIOS e password di rete, trimestralmente cambiate.

Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione contabili dei dipendenti e degli alunni) sono ubicate in modo tale che ciascun addetto possa rilevare a vista e impedire il tentativo di accesso da parte di persone estranee.

Sono state impartite disposizioni affinché, in assenza del personale, le stanze rimangano chiuse e le chiavi siano custodite dal personale collaboratore scolastico in servizio addetto alla

vigilanza che, al termine del servizio, provvederà al deposito delle chiavi nell'apposito contenitore.

L'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Di seguito si illustrano le norme applicate per garantire la sicurezza e l'integrità dei dati per:

- *Computer e supporti informatici*: I computer, inclusi i server, risultano tutti sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti; il server è collegato ad un gruppo di continuità che consente di escludere al perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica. L'integrità dei dati sul server amministrativo è garantita da una doppia procedura di backup: la prima avviene in automatico con apposito software che giornalmente opera il salvataggio di una copia dei dati sul server stesso; la seconda è effettuata normalmente masterizzando su CD ROM ogni sabato, i backup di tutta la settimana eseguiti sul server. I CD ROM vengono conservati per almeno due mesi nell'apposta cassaforte ignifuga e stagna alle infiltrazioni di acqua. Titti i server della rete amministrativa vengono protetti da password per impedire al personale non autorizzato l'accesso alla rete amministrativa. Le password sono assegnate e riportate su un apposito foglio conservato nella cassaforte collocata della stanza del DSGA. L'introduzione di password di BIOS all'accensione dei personal computer, di password dello screen-saver e di password per l'accesso in rete determina un soddisfacente livello di protezione dei dati contenuti nei PC. L'introduzione delle password e di apposito software antivirus inibisce ad estranei l'uso dei personal computer, attraverso i quali, tramite Proxy, si accede alla posta elettronica.
- Per l'invio di messaggi e-mail a più destinatari, sono state fornite al personale istruzioni affinché quale destinatario venga sempre indicata la scuola con l'indirizzo e-mail e in CCN i destinatari, in modo che non possano essere individuati gli indirizzi e-mail degli altri destinatari attraverso la funzione di proprietà.

  I CD ROM masterizzati contenenti copie degli archivi eseguiti localmente dai computer sono custoditi negli appositi contenitori di plastica e inseriti nella cassaforte sempre chiusa con combinazione alfanumerica su serratura elettronica. I floppy disk contenenti dati degli studenti, delle famiglie degli stessi, dei lavoratori dipendenti e collaboratori, possono essere riutilizzati esclusivamente dopo opportuna formattazione, in modo da impedire la lettura dei dati precedenti, cosi come stabilito dalla legge. I CD ROM non più utilizzabili vengono distrutti.

  I floppy disk contenenti dati, prima della formattazione, sono custoditi nello stesso modo dei DVD contenenti copie degli archivi. Per quanto riguarda infine l'obbligo previsto dalle misure minime sulla sicurezza di cui all'allegato B del codice della privacy, i computer sono dotati di programma antivirus che è aggiornato sotto la responsabilità del titolare del trattamento a cadenza almeno trimestrale e che consente di rilevare immediatamente all'apertura di un file la presenza di un virus.

- *Supporti cartacei:* relativamente ai supporti cartacei sono state impartite dettagliate istruzioni a tutto il personale al momento dell'affidamento dell'incarico e nel corso degli interventi di formazione. (vedi lettere di individuazione degli incaricati del trattamento dei dati e Linee Guida allegate)
- *Gestione della privacy e trattamento dei dati raccolti attraverso il sito Web*

  Si rimanda all'informativa sui diritti dell'utente che accede al sito web della scuola, pubblicato sul sito: www._____ e allegato al presente DPS.

Tabella 4.1 – Le misure di sicurezza adottate o da adottare (regola 19.4 del disciplinare tecnico)

Id Misura	*Misura*	*Descrizione dei rischi contrastati*	*Trattamenti interessati*	*Misura già in essere*	*Misura da adottare*	*Struttura o persone addette all'adozione*
M1	**Predisposizione dei profili di autorizzazione di accesso agli applicativi Axios**	**R1,R2,R3, R4**	**T7**	X		**A4 – Amministratore di Sistema**
M2	**Procedura formale di concessione delle credenziali per l'utilizzo degli applicativi Axios**	**R1,R2,R3, R4**	**T7**	X		**A4 – Amministratore di Sistema**
M3	**Procedura per la concessione di credenziali per l'accesso all'area riservata di Istruzione.it**	**R1,R2,R3, R4**	**T7**	**X**		**A3.2 – Ufficio DSGA**
M4	**Concessione delle credenziali per l'accesso a SIMPI**	**R1,R2,R3, R4**	**T7**	**X**		**A3.2 – Ufficio DSGA**
M5	**Concessione credenziali per la gestione della posta elettronica**	**R1,R2,R3, R4**	**T10**	**X**		**A3.2 – Ufficio DSGA**
M6	**Concessione delle credenziali per l'accesso all'applicativo per le denunce di infortunio alunni della Regione Lazio**	**R1,R2,R3, R4**	**T1**	**X**		**A3.2 – Ufficio DSGA**
M7	**Concessione credenziali accesso sito rilevazione scioperi**	**R1,R2,R3, R4**	**T11**	**X**		**A3.2 – Ufficio DSGA**

M8	**Concessione delle credenziali per l'accesso al sito Anagrafe Prestazioni**	**R1,R2,R3, R4**	**T14**	**X**		**A3.2 – Ufficio DSGA**
M9	**Concessione delle credenziali per l'accesso al sito Entratel**	**R1,R2,R3, R4**	**T13**	**X**		**A3.2 – Ufficio DSGA**
M10	**Concessione delle credenziali per l'accesso alla spedizione telematica del DM10**	**R1,R2,R3, R4**	**T13**	**X**		**A3.2 – Ufficio DSGA**
M11	**Concessione delle credenziali per l'accesso al servizio di invio de conguaglio fiscale**	**R1,R2,R3, R4**	**T13**	**X**		**A3.2 – Ufficio DSGA**
M12	**Concessione delle credenziali per l'accesso ai dispositivi di amministrazione del sistema informativo**	**R1,R2,R3, R4, R8,R9**	**T4**	**X**		**A4 – Amministratore di Sistema**
M13	**Concessione delle credenziali per l'accesso di ciascun utente del sistema alle risorse de dominio**	**R1,R2,R3, R4**	**T7**	**X**		**A4 – Amministratore di Sistema**
M14	**Installazione Antivirus sui PC della rete Amministrativa**	**R5,R6**	**T7**	**X**		**A4 – Amministratore di Sistema**
M15	**Redazione di un disciplinare tecnico per le procedure**	**R5,R7,R11, R12,R13**	**T7**	**X**		**A4 – Amministratore di Sistema**

	di Backup con cadenza almeno settimanale					
M16	**Verifica delle procedure di ripristino di Backup**	**R5,R7,R11,R12, R13**	**T7**	X		**A4 – Amministratore di Sistema**
M17	**Configurazione o ripristino del sistema operativo dei clients**	**R1,R2,R3, R4**	**T7**	**X**		**A4 – Amministratore di Sistema**
M18	**Redazione di un disciplinare tecnico per la conservazione dei supporti di memorizzazione removibili**	**R5,R7,R11, R12,R13**	**T7**	**X**		**A4 – Amministratore di Sistema**
M19	**Predisposizione di un piano di interventi di manutenzione dell'Hardware al fine di garantire l'integrità dei dati**	**R7**	**T7**	**X**		**A4 – Amministratore di Sistema**
M20	**Procedura di concessione delle autorizzazioni all'accesso dei documenti cartacei**	**R10,R13**	**T27**	**X**		**A3.2 – Ufficio DSGA**
M21	**Impianto del registro degli accessi ai locali dell'ufficio dopo l'orario di chiusura**	**R10,R13**	**T27**	**X**		**A3.2 – Ufficio DSGA**
M22	**Installazione nei locali in cui sono contenuti gli archivi informatici e cartacei di**	**R10,R13**	**T24**	**X**		**A4 – Amministratore di Sistema**

	un impianto antifurto					
M23	**Predisposizione di armadi provvisti di chiusura per la custodia dei documenti**	**R10,R13**	**T24**	**X**		**A4 – Amministratore di Sistema**
M24	**Procedura formale di consegna delle chiavi degli armadi agli incaricati dei trattamenti**	**R10,R13**	**T7**	**X**		**A3.2 – Ufficio DSGA**
M25	**Procedura formale di concessione delle autorizzazioni per l'accesso ai locali**	**R10,R13**	**T7**	**X**		**A3.2 – Ufficio DSGA**

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°1		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M1**				
Descrizione sintetica	**Predisposizione dei profili di autorizzazione di accesso agli applicativi Axios**				
Elementi Descrittivi	Tramite il programma di gestione sicurezza di AXIOS SOFTWARE, assegnazione all'utente identificato dal DSGA di nome utente e password per l'accesso al software specifico di lavoro. L'accesso al software SICUREZZA AXIOS è consentito all'amministratore di sistema.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°2		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M2**				

Descrizione sintetica	**Procedura formale di concessione delle credenziali per l'utilizzo degli applicativi Axios**	
Elementi Descrittivi	Comunicazione da parte del DSGA del nome dell'utente e dell'applicativo che andrà ad utilizzare. Scelta della password usata per l'accesso. La password viene comunicata all'utente in busta chiusa con il nome utente utilizzato per l'accesso. L'elenco completo delle password è custodito in apposita cassaforte accessibile tramite codice di accesso.	
Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°3		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M3**				
Descrizione sintetica	**Procedura per la concessione di credenziali per l'accesso all'area riservata di Istruzione.it**				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°4		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M4**				
Descrizione sintetica	**Concessione delle credenziali per l'accesso a SIMPI**				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				

Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°5		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M5**				
Descrizione sintetica	**Concessione credenziali per la gestione della posta elettronica**				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°6		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M6**				
Descrizione sintetica	**Concessione delle credenziali per l'accesso all'applicativo per le denunce di infortunio alunni della Regione Lazio**				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°7		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M7**				
Descrizione sintetica	**Concessione credenziali accesso sito rilevazione scioperi**				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°8		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M8**				
Descrizione sintetica	**Concessione delle credenziali per l'accesso al sito Anagrafe Prestazioni**				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°9		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M9**				
Descrizione sintetica	**Concessione delle credenziali per l'accesso al sito Entratel**				
Elementi Descrittivi	Le credenziali per l'accesso al sito ENTRATEL vengono concesse dal servizio ministeriale dell'Agenzia delle Entrate. Il DSGA individuato l'operatore consegna le credenziali di accesso.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°10		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M10**				
Descrizione sintetica	**Concessione delle credenziali per l'accesso alla spedizione telematica del DM10**				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°11		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M11**				
Descrizione sintetica	**Concessione delle credenziali per l'accesso al servizio di invio de conguaglio fiscale**				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°12		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M12**				
Descrizione sintetica	**Concessione delle credenziali per l'accesso ai dispositivi di amministrazione del sistema informativo**				
Elementi Descrittivi	Il Dirigente scolastico e il DSGA individua tra il personale interno, in possesso delle relative competenze informatiche, la persona che amministra il sistema.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°13		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M13**				
Descrizione sintetica	**Concessione delle credenziali per l'accesso di ciascun utente del sistema alle risorse de dominio**				

Elementi Descrittivi	E' stato creato un profilo comune di rete generico. Le credenziali concesse sono tali da non recare nessun tipo di accesso deleterio per i dati archiviati.	
Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°14		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M14**				
Descrizione sintetica	**Installazione Antivirus sui PC della rete Amministrativa**				
Elementi Descrittivi	Il software antivirus è installato singolarmente sia sul server che sui clients. L'aggiornamento del l'antivirus viene effettuato in automatico via internet.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°15		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M15**				
Descrizione sintetica	**Redazione di un disciplinare tecnico per le procedure di Backup con cadenza almeno settimanale**				
Elementi Descrittivi	Il Backup del database viene effettuato in automatico da un apposito software installato sul server di rete, lo stesso effettua anche il ripristino del database.La copia del bck viene archiviata in una cartella di sistema del server. La cadenza del bck è giornaliera, un' ulteriore copia del bck viene effettuata ogni sette giorni su supporto magnetico dvd/cd che viene conservato per due mesi nella apposita cassaforte ignifuga in dotazione.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°16		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M16**				
Descrizione sintetica	**Verifica delle procedure di ripristino di Backup**				

Elementi Descrittivi	Ogni settimana, con il programma gestionale AXIOS BACKUP e RESTORE viene simulato un ripristino del database sia con la copia presente nella cartella di sistema sia con la copia archiviata su supporto magnetico.	
Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°17		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M17**				
Descrizione sintetica	**Configurazione o ripristino del sistema operativo dei clients**				
Elementi Descrittivi	Ogni clients è fornito all'origine di disco di ripristino del sistema operativo. In caso di danneggiamento del sistema un tecnico ATA individuato e incaricato con apposito provvedimento reinstalla e riconfigura le funzionalità dell'apparecchio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°18		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M19**				
Descrizione sintetica	**Predisposizione di un piano di interventi di manutenzione dell'Hardware al fine di garantire l'integrità dei dati**				
Elementi Descrittivi	La verifica del funzionamento hardware è fatta con cadenza annuale. Le verifiche vengono effettuate sul server di rete SISSI. Sul server SISSI è installato il data base generale dei dati sia didattici che sensibili. La verifica principale consiste nel testare l'efficienza dei lettori cd-rom e l'integrità del Hard-disk.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°19		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M20**				

Descrizione sintetica	**Procedura di concessione delle autorizzazioni all'accesso dei documenti cartacei**	
Elementi Descrittivi	Il DSGA individua, in base ai compiti assegnati ad ogni assistente amministrativo, la concessione ad accedere ai relativi archivi cartacei.	
Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°20		***Compilata da DSGA***		***Data di compilazione (Modifica)***	14 dicembre 2005
Misura	**M23**				
Descrizione sintetica	**Predisposizione di armadi provvisti di chiusura per la custodia dei documenti**				
Elementi Descrittivi	Ogni Assistente Amministrativo assegnato all'ufficio preposto e tenuto alla conservazione dei documenti negli appositi armadi provvisti di serratura con chiave.				
Data di aggiornamento	15 marzo 2007				

5 Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Al fine di garantire il ripristino dei dati in seguito a distruzione o danneggiamento, l'istituzione scolastica dispone di idonee procedure di salvataggio periodico (backup) che consistono nell'utilizzo dell'apposito software di backup del programma di gestione amministrativo il quale crea in automatico una copia compressa dei dati, archiviandoli in un'apposita cartella del server, e di un masterizzatore DVD che salva i dati anche su disco DVD registrabile, da utilizzarsi giornalmente al termine dell'orario lavorativo.

Tabella 5.1 – Criteri e procedure per il ripristino della disponibilità dei dati (regola 19.5 del disciplinare tecnico)

Ripristino		
Banca dati / archivio dati	***Criteri e procedure per il salvataggio e il ripristino dei dati***	***Pianificazione delle prove di ripristino***
DATABASE SISSI	**In automatico con il software di gestione amministrativo AXIOS con cadenza giornaliera**	**Quindicinale**

Documenti di Office application	**E' stata predisposta una attività pianificata sul pc dell'utente di una masterizzazione della cartella documenti**	**Quindicinale**
Documenti Posta elettronica	**E' stata predisposta una attività pianificata sul PC utilizzato per la posta elettronica di masterizzazione dei dati di posta**	**Quindicinale**

Tabella 5.2 – Criteri e procedure per il salvataggio dei dati (regola 19.5 del disciplinare tecnico)

Salvataggio			
Banca dati	***Criteri e procedure per il salvataggio***	***Luogo di custodia delle copie***	***Struttura o persona incaricata del salvataggio***
Server Supporto Magnetico DVD	**Software applicativo axios automatizzato Copia archivi su DVD registrabile**	***Cassaforte Ignifuga e a tenuta stagna***	**Amministratore di Sistema**

6 Previsione di interventi formativi degli incaricati del trattamento

Gli interventi formativi sono programmati nell'ambito del piano di formazione e aggiornamento del personale, con cadenza annuale, per rendere gli incaricati del trattamento edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. Sono previste idonee attività di formazione in occasione di innovazioni e/o modifiche delle norme e in relazione allo sviluppo scientifico/tecnologico dei mezzi e dei sistemi di protezione.
La formazione è altresì programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. L'incarico al trattamento dei dati contiene, oltre alle istruzioni date dal responsabile, anche le linee guida per il trattamento dei dati, le informazioni relative al significato dei termini e le schede allegate al Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione . Gli incaricati partecipano alla riunione annuale per la verifica e la revisione del documento programmatico per la sicurezza. Verrà valutata l'eventuale partecipazione del personale della scuola alle iniziative formative organizzate dall'USR del Lazio.

Tabella 6 – Pianificazione degli interventi formativi previsti (regola 19.6 del disciplinare tecnico)

Descrizione sintetica degli interventi formativi	***Classi di incarico o tipologie di incaricati interessati***	***Tempi previsti***
Attuazione delle norme sulla riservatezza dei dati personali – Acquisizione di competenze giuridiche e di organizzazione scolastica – Responsabilità dei docenti nel trattamento dei dati personali con	Docenti incaricati del trattamento dei dati personali	1 ore di attività di formazione in un incontro di 1 ora – a.s. 2006/07

riferimento al REGOLAMENTO sul trattamento dei dati sensibili e giudiziari		
Miglioramento dell'attuazione delle norme sulla riservatezza dei dati personali nella scuola	Personale ATA della scuola	2 ore di attività di formazione– a.s. 2006/07

7 Descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare

Dati personali sono gestiti dal sistema informativo del MPI che non ha ancora comunicato le misure adottate e alcun documento programmatico.

8 Individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale (Regola 19.8 del disciplinare tecnico)

Pur non rientrando fra gli organismi tenuti alla attuazione del punto 24, l'istituzione scolastica ha messo in atto particolari misure di protezione nell'archiviazione dei dati personali idonei a rivelare lo stato di salute, conservandoli sempre in busta chiusa inserita all'interno del fascicolo personale.

9 Conclusioni

Il presente documento sarà tempestivamente aggiornato nel caso di sostituzione di attrezzature o di cambiamenti nella disposizione degli spazi di lavoro e, in ogni caso, entro il 31 marzo di ciascun anno.

Agli incaricati del trattamento è stata data informazione circa il contenuto del presente documento, attraverso la consegna di una copia , con rilascio di ricevuta dell'avvenuta consegna, nella quale si dà atto della comunicazione dell'obbligo di uniformarsi al documento.

Il responsabile del trattamento è tenuto a vigilare sull'osservanza delle disposizioni stesse da parte degli incaricati e a emanare ulteriori disposizioni relative alla gestione della sicurezza dei dati.

Il presente documento è stato illustrato nel corso di apposite riunioni, tenute in orario di lavoro, alle quali hanno partecipato il Dirigente Scolastico, il responsabile del trattamento ed il personale ATA incaricato del trattamento, nel rispetto delle disposizioni del D.Lgs 196/03 che prevede l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.
In occasione delle riunioni, che saranno successivamente previste per la formazione, si provvederà anche alla valutazione ed alla revisione delle misure di sicurezza.

Le attività di formazione del personale incaricato e di revisione del presente documento vengono annotate in apposito registro verbale tenuto dal Responsabile del trattamento.
Il presente documento è stato illustrato ai docenti nella riunione del Collegio dei Docenti del _____, con particolare riferimento a quanto attiene alle

documentazioni ed ai dati personali che vengono consegnati agli stessi e alle istruzioni date ai docenti incaricati del trattamento dei dati.

Data 15 marzo 2007

Il titolare del trattamento
IL DIRIGENTE SCOLASTICO

Da www.paginescuola.it

1) **Comunicato del Garante alle scuole, con importante punto sul regolamento (3.12.2004) (Pag. 20)**
2) **Decisione del Garante riguardo a una scuola (24.4.2005) (Pag. 21)**

Finalmente il Garante fa chiarezza su alcuni punti che ci riguardano !

A PROPOSITO DEL REGOLAMENTO PREVISTO DALL'ART. 20-21-22

Per quanto riguarda, infine, supposti regolamenti privacy da adottare da parte delle scuole, nessun istituto scolastico secondario dovrà o potrà dotarsi a proprio piacimento di un regolamento sui dati "sensibili". Il "Codice" contiene già regole chiare e ciò che manca al riguardo è solo un unico regolamento attuativo ministeriale che dovrà conformarsi ad un parere del Garante.

La *privacy* ha costituito a volte il pretesto per improprie note di colore o è stata utilizzata come un alibi per non applicare altre disposizioni di legge. Una corretta informazione è quindi importante.

(EMESSO 3.12.2004)

Garante Privacy

(emesso 3.12.2004).

"Molte falsità sulla privacy a scuola".

1. "*Non è vero che i voti scolastici devono restare segreti*"

2. "*non è vero che gli studenti devono 'nascondere' la propria fede religiosa*, "

3. "*non è vero che i risultati degli scrutini devono rimanere clandestini*".

Secca smentita del Garante alle notizie del tutto infondate riguardanti la privacy nelle scuole.

Notizie che, nonostante le pronte e numerose precisazioni del Garante, non smettono di essere riportate anche da quotidiani a carattere nazionale, senza le necessarie verifiche.

L'Autorità (Stefano Rodotà, Giuseppe
Santaniello, Gaetano Rasi, Mauro Paissan) ritiene, dunque, doveroso chiarire in maniera decisa ancora una volta che tali notizie non sono vere.

Siamo di fronte a una vera e propria leggenda metropolitana.

Non esiste alcun provvedimento del Garante che imponga di tenere segreti i voti dei compiti in classe, delle interrogazioni o gli scrutini, né di consegnarli agli alunni in busta chiusa.

Mai, in nessun caso, un tale provvedimento è stato preso, né, tanto meno, esso è previsto dall'attuale legge in vigore, il Codice in materia di tutela dei dati personali entrato in vigore il primo gennaio di quest'anno.

Dal 1997 il Garante si sforza, anche con comunicati stampa, di ricordare che i risultati degli scrutini – che non sono, peraltro, dati sensibili, soggetti a speciali tutele - **devono essere al contrario pubblicati** anche dopo l'avvento della normativa sulla privacy, essendo ciò previsto da una specifica disciplina in materia e rispondendo a principi di trasparenza.

Il 9 febbraio di quest'anno, un'ordinanza del Ministro per l'istruzione
ricorda peraltro che anche i punteggi attribuiti come crediti scolastici a ciascun alunno sono pubblicati nell'albo degli istituti, unitamente ai voti conseguiti in sede di scrutinio finale. In ciascun albo va anche pubblicato l'esito degli esami, "con la sola indicazione della dizione non promosso nel caso di esito negativo".

Analoghe soluzioni sono state indicate in passato in varie ordinanze ministeriali del 2001 e del 2003 .

Così come non esiste alcun provvedimento del Garante che proibisce agli alunni di rendere nota la fede religiosa o che ostacola le soluzioni da tempo in atto per la partecipazione o meno degli alunni all'ora di religione.

Il necessario rispetto della volontà di ciascuno di mantenere
riservate alcune informazioni sulla propria persona, infatti, non va confusocon la libertà, costituzionalmente protetta, di ognuno di manifestare liberamente le proprie convinzioni, anche di natura religiosa.

Per quanto riguarda, infine, supposti regolamenti privacy da adottare da parte delle scuole, nessun istituto scolastico secondario dovrà o potrà dotarsi a proprio piacimento di un regolamento sui dati "sensibili". Il "Codice" contiene già regole chiare e ciò che manca al riguardo è solo un unico regolamento attuativo ministeriale che dovrà conformarsi ad un parere del Garante.

La privacy ha costituito a volte il pretesto per improprie note di colore oè stata utilizzata come un alibi per non applicare altre disposizioni di legge.

Una corretta informazione è quindi importante.

** Tratto dal Comunicato stampa del Garante datato:

Roma, 3 dicembre 2004

Pubblicazione del Garante Privacy in data 24 aprile 2005

Questionari a scuola e garanzie per alunni e genitori

Il Garante blocca la pubblicazione di una tesi di laurea perché i dati erano stai raccolti in modo illecito

Bloccati dal Garante per trattamento illecito di dati personali alcuni risultati di una ricerca universitaria, svolta in una scuola elementare e riportati in una tesi di laurea in via di pubblicazione. Gli alunni, e di conseguenza i genitori, non erano stati informati né degli scopi dell'iniziativa, né del fatto che la loro partecipazione era facoltativa e non obbligatoria.

Il provvedimento di blocco adottato alcune settimane or sono dall'Autorità (della quale è stato di recente nominato presidente Francesco Pizzetti) riguarda le informazioni personali, in alcuni casi anche sensibili, raccolte tramite questionari sottoposti ad alcuni alunni delle elementari o elaborate nelle varie fasi della ricerca, con esclusione dei dati aggregati e anonimi. A seguito del provvedimento l'Università, titolare della ricerca, non ha potuto utilizzare più queste informazioni dovendo limitarsi alla sola conservazione.

La vicenda ha inizio quando i genitori di un alunno delle scuole elementari hanno saputo che il figlio di sette anni ha partecipato, a loro insaputa, ad una ricerca sulla rappresentazione sociale del maltrattamento infantile. La rilevazione, autorizzata dal dirigente dell'istituto scolastico, ha coinvolto gli alunni di alcune classi elementari ai quali una laureanda ha sottoposto questionari a risposta multipla e vignette. La ricerca ha comportato il trattamento di diverse informazioni (sesso, età, classe e scuola frequentata, mese ed anno di nascita) e pur non comprendendo il nome e il cognome degli alunni che vi hanno preso parte, permette, visto il ristretto ambito di indagine e grazie alla loro interazione, una agevole identificazione. Diversi minori, inoltre, hanno inserito la data di nascita completa (giorno, mese ed anno) rendendo ancora più semplice la loro identificabilità. Alcune delle informazioni richieste, infine, erano riconducibili alla nozione di dato sensibile in quanto idonee a rivelare aspetti della sfera psico-fisica dei genitori.

Procedura illegittima e possibile violazione della privacy secondo i genitori dell'alunno, i quali si sono correttamente rivolti all'Università, lamentando anzitutto di non essere stati informati della ricerca e di non aver manifestato il loro consenso alla partecipazione, chiedendo poi di accedere ai dati personali contenuti nei questionari compilati dal figlio e opponendosi infine al loro ulteriore trattamento. Insoddisfatti della risposta ricevuta hanno presentato ricorso al Garante.

Dal canto suo l'università, nel sostenere legittimità del proprio operato, ha dichiarato di non poter consentire l'accesso dei genitori ai questionari del figlio non conoscendo i dati anagrafici dei minori sottoposti alle prove. Il trattamento dei dati personali poi, secondo l'ente, era avvenuto nell'esercizio delle proprie funzioni istituzionali e solo dopo il consenso del dirigente scolastico.

Il Garante ha invece ritenuto illecito il trattamento dei dati personali e, a tutela dei soggetti coinvolti, ne ha disposto il blocco. Per poter svolgere legittimamente la rilevazione, infatti, l'università, operando per finalità di ricerca, avrebbe dovuto informare correttamente i genitori degli

scopi dell'iniziativa e del fatto che la partecipazione dei bambini era non obbligatoria, ma volontaria. L'università ha quindi posto in essere un trattamento illecito di dati personali e per questo motivo le informazioni raccolte non sono utilizzabili.

Recite scolastiche e privacy

L'Autorità Garante per la protezione dei dati personali ha precisato che l'uso di videocamere o macchine fotografiche per documentare eventi scolastici e conservare ricordi dei propri figli non ha ovviamente niente a che fare con le norme sulla privacy.

Si tratta, infatti, di immagini non destinate a diffusione, ma raccolte per fini personali e destinate ad un ambito familiare o amicale: il loro uso è quindi del tutto legittimo.

L'intervento del Garante si è reso necessario perché già diverse sono le segnalazioni giunte agli uffici dell'Autorità per un chiarimento su questo aspetto, considerato che in alcune scuole viene vietato a genitori e familiari di fare riprese e foto dei propri bambini.

La formazione: un ineliminabile presupposto della sicurezza.

Il punto 19.6 del Disciplinare Tecnico, allegato B al Codice della Privacy, dispone "*…la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali*".

La sicurezza dei dati personali non è esclusivamente affidata alle misure si sicurezza logiche (antivirus, password…) o fisiche (lucchetti, sistemi di videosorveglianza…) ma anche e principalmente all'attenzione dell'operatore che quotidianamente si trova a gestirli e "trattarli".

E' inutile, infatti, dotare l'azienda o l'ente dei più sofisticati sistemi di protezione se non si forma il personale sui pericoli e sulle responsabilità, civili e penali, derivanti da una cattiva custodia dei dati o da un loro illecito trattamento.

Per questo motivo il programma di formazione deve essere costantemente aggiornato alla luce delle più rilevanti novità normative, delle decisioni della giurisprudenza e dei provvedimenti del Garante per la protezione dei dati personali.

La conoscenza dei pericoli e delle norme del Codice della Privacy diviene così il necessario presupposto per la sicurezza dei dati personali.

La formazione: requisiti e modalità di attuazione.

Dalla lettura del Codice della Privacy e del Disciplinare Tecnico (all.B) si evince chiaramente che la formazione deve necessariamente essere:
a) adeguata alle specifiche esigenze lavorative ed ambientali del sistema di trattamento dei dati;
b) idonea a trasmettere agli incaricati e/o responsabili le nozioni necessarie relative alle misure minime di sicurezza disposte dal titolare ai sensi del suddetto Codice;
c) tempestiva ed efficace, secondo quanto normativamente disposto, all'ingresso in servizio, ad ogni cambiamento di mansione, ad ogni introduzione di nuove tecnologie e procedure operative;

d) formale, in quanto il momento formativo deve essere menzionato nel documento programmatico sulla sicurezza e certificato dagli addetti.

Programma

Il programma, in base al *target* di riferimento (ad esempio: area amministrativa, area legale, area risorse umane…), dovrà essere svolto a vari livelli di approfondimento e con diverse modalità di approccio didattico.

Descrizione per punti di un programma "tipo":

Norme e Principi generali:

- Analisi delle vigenti disposizioni di legge con la fornitura del materiale di supporto;
- Breve introduzione alla criminalità informatica ;
- Fonti normative comunitarie in materia di trattamento di dati personali;
- Il Decreto legislativo n. 196/2003 "Codice in materia di trattamento dei dati personali" - esame generale;
- Analisi del Disciplinate Tecnico in materia di misure minime di sicurezza;
- Profilo dei soggetti coinvolti nella tutela dei dati personali e delle loro responsabilità;
- Principi di diligenza secondo il codice civile: i profili di responsabilità penale e civile.
- L'inversione dell'onere della prova.
- Il Titolare: condizioni di efficacia e validità della delega al responsabile
- Gli adempimenti principali del Codice della privacy.
- Analisi approfondita degli apprestamenti di sicurezza, sia a livello di misure minime che di misure appropriate.

Disposizioni e misure tecniche:

- Principi di sicurezza logica e fisica dei sistemi informativi;
- Misure di prevenzione e di contenimento del danno;
- La protezione dei centri di elaborazione dati: difese fisiche, elettroniche e procedurali;
- Strumenti di protezione hardware e software ;
- Contenitori di sicurezza ;
- Sistemi antintrusione e sistemi di controllo dell'accesso fisico (serrature, chiavi e loro gestione);
- Sistemi di spegnimento incendi;
- Procedure di creazione, gestione, conservazione e trasporto di copie di Back Up;
- I comportamenti preventivi e le procedure di emergenza;
- Il controllo dell'accesso fisico ;

- Gli applicativi di controllo dell'accesso logico: applicativi di controllo dell'acceso logico a dati e programmi;
- Sistemi di autenticazione e di autorizzazione;
- Particolari precauzioni nel trattamento di dati sensibili e giudiziari.

Riepilogo e Sintesi

Perché è necessaria la formazione del personale in ambito aziendale (pubblico e privato) in materia di trattamento dei dati personali (Privacy)?

Il Codice in materia di protezione dei dati personali (D.Lgs. 196/2003) impone l'adozione, attraverso la previsione di specifiche sanzioni amministrative e penali, di una serie di misure tecniche, informatiche, organizzative, logistiche e procedurali tendenti a realizzare un livello di sicurezza proporzionato ai rischi dell'attività, privata o pubblica, esercitata. In questa prospettiva la formazione del personale occupa un ruolo strategico di primaria rilevanza.

Quali soggetti sono obbligati al rispetto delle norme in materia di trattamento dei dati personali (Privacy) ?

Sono obbligati al rispetto delle suddette regole tutti coloro che trattano dati personali, a titolo esemplificativo: aziende, liberi professionisti (avvocati, commercialisti, medici...), pubbliche amministrazioni, enti ospedalieri, istituti scolastici; enti territoriali (regioni, province, comuni)…

- Documento redatto dal dott. Leo Stilo

Una misura di sicurezza obbligatoria: la formazione degli addetti al trattamento dei dati

Per la protezione dei dati e della privacy **è il fattore umano che quasi sempre determina i rischi maggiori**. Capita spesso che le password dei computers siano puerilmente facili da indovinare, quando non sono scritte in un foglietto visibile da chiunque. Dischetti sono lasciati in giro e chiunque potrebbe intascarli e leggerli. Documenti anche delicati sono lasciati in bella vista. Al telefono vengono date informazioni che non si ha diritto di comunicare oppure vengono date a persone che non hanno diritto di riceverle o che almeno andrebbero prima identificate con certezza. E così via. Ogni operatore, a qualsiasi livello, è esposto al rischio di distrazioni, imprudenze, errori da faciloneria o pigrizia, etc. E'

inutile implementare sofisticati sistemi di protezione dei dati se l'operatore non fa la sua parte. Per esempio, un programma antivirus serve a poco se non è aggiornato quotidianamente o, al massimo, settimanalmente, contro le decine di nuovi virus che vengono messi in circolazione ogni giorno. E' fondamentale che l'operatore ne sia consapevole e conosca i gravissimi rischi connessi. E via dicendo.

Obblighi derivanti dal Codice

Il Codice Privacy tratta della formazione nell' Allegato B, contenente il Disciplinare tecnico in materia di misure minime di sicurezza. La regola 19.6 prevede infatti interventi formativi degli incaricati, per renderli edotti di una serie di argomenti. La stessa regola stabilisce che la formazione deve essere programmata:

- all'inizio dell'applicazione del Codice Privacy
- al momento dell'ingresso in servizio di un nuovo addetto
- in occasione di cambiamenti di mansioni
- in caso di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati
-

Inoltre, nel Documento Programmatico sulla Sicurezza (DPS) è obbligatorio indicare le misure di sicurezza adottate e, fra queste, gli interventi formativi previsti per preparare il personale all'applicazione di tali misure.

Come premesso, la regola 19.6 è una delle misure minime di sicurezza obbligatorie, quindi l'omissione costituisce reato penale (arresto fino a 2 anni o ammenda da € 10.000 a € 50.000).

E' vero che questa regola si riferisce agli Incaricati che utilizzano il computer, però si noti che la normativa su tutti gli Incaricati (art. 30) prevede che la loro nomina sia **accompagnata da adeguate istruzioni**. E' evidente che un Incaricato al quale non siano stati spiegati il quadro normativo generale, i rischi a cui i dati sono sottoposti e le misure da applicare, nonché la ragione di tutto questo, non sarà né motivato, né all'altezza della sua funzione. Nel caso che commetta un errore o una violazione, potrà sempre invocare la scusante di non aver avuto una formazione sufficiente.

Requisiti della formazione.

In conclusione, la lettura combinata delle varie disposizioni del Codice porta a definire i seguenti requisiti. **Ogni addetto deve ricevere adeguata formazione**:

- di tipo generale sulla disciplina della protezione dei dati personali, ma specialmente focalizzata sugli aspetti più rilevanti in rapporto all'attività da lui svolta
- sulle responsabilità che ne derivano
- sui rischi che incombono sui dati e in particolare sui rischi specifici relativi alla sua mansione
- sulle misure disponibili per prevenire/evitare eventi dannosi ed in particolare su quelle specifiche della sua mansione
- sulle modalità per aggiornarsi sulle misure di sicurezza adottate dal titolare (si noti che il DPS va integrato al 31 marzo di ogni anno con i miglioramenti progressivi delle misure di sicurezza e dell'organizzazione, quindi al dipendente va spiegato

cos'è e come si legge il DPS)

Oltre a quella iniziale, va obbligatoriamente fornita formazione:

- integrativa in caso di cambio di mansione
- integrativa in caso di introduzione di nuove tecnologie o nuove misure di sicurezza che abbiano impatto significativo sul trattamento dei dati
- rinnovata e completa in caso di nuovo assunto (vale anche per i lavoratori temporanei o supplenti).

Come si vede è quasi **un vestito su misura** per ciascuna categoria di Incaricati. E a volte **un vestito su misura per il singolo**, in quanto svolga mansioni particolari o abbia particolari responsabilità in ambito privacy (esempio: custode delle password, amministratore di sistema, ecc.).

E' anche quasi indispensabile, benché non obbligatoria, la programmazione di una sorta di formazione permanente, per due buone ragioni: a) durante l'attività concreta s'incontrano nuovi problemi e difficoltà organizzative, pertanto è opportuno valutarli e prendere adeguati provvedimenti; 2) col tempo si affievolisce la motivazione che è alla base di un valido comportamento, quindi è assolutamente indispensabile prevedere momenti di aggiornamento e riflessione che "ricarichino" il personale.

Infine, non vanno dimenticate le esigenze di formazione dei Responsabili e del rappresentante del Titolare. Per loro il Codice Privacy non prescrive obblighi formativi, essendo impliciti nel loro ruolo. Ma essi si trovano in una posizione delicata e scomoda, per cui devono avere una buona formazione generale e a volte anche specifica sui singoli argomenti, in quanto il Codice Privacy prevede che diano adeguate istruzioni agli Incaricati e pone sulle loro spalle la pesante **responsabilità oggettiva del comportamento dei loro sottoposti e di quanto accade ai dati personali**.

Va sottolineato il requisito della **documentabilità**, perché – essendo una misura di sicurezza obbligatoria - in caso di controllo (casuale o a seguito di un esposto) viene richiesta la prova dell'applicazione.

Requisiti dei formatori

Il Codice Privacy non stabilisce chi ha titolo per eseguire la formazione, né prevede particolari forme attuative, però pretende il risultato dal Titolare e dai Responsabili. Se ne deduce che essi sono liberi di utilizzare qualsiasi modalità, purché sia adeguata a produrre l'effetto richiesto.

Il formatore potrà quindi essere lo stesso titolare o il Responsabile, se hanno capacità e conoscenza idonee. Mentre è probabile che essi abbiano molta capacità e buone conoscenze, è improbabile che possano sobbarcarsi l'intero peso della formazione nei suoi vari aspetti, specificazioni per tipologie di Incaricati, tempi.

L'uso di formatori esterni che vengano in azienda a tenere corsi e riunioni è sicuramente utile per la parte generale che – più o meno – può andare bene per tutti gli Incaricati, anche se appare francamente difficile che uno stesso corso possa rivolgersi contemporaneamente a persone che hanno capacità di apprendimento molto differenziate (quali gli uscieri o bidelli a fronte dei funzionari laureati) ed esigenze conoscitive assai diverse. La stessa difficoltà s'incontra mandando i dipendenti a corsi esterni; in più, c'è la

quasi impossibilità di mandare tutti. Il difetto di questi corsi, interni o esterni che siano, è che restano generici e non possono calarsi sull'effettiva organizzazione privacy dell'Azienda o dell'Ente.

Infine, non va sottovalutato il problema dei costi ingenti di una formazione effettuata con questi strumenti e per **tutti** gli incaricati, adattandola a ciascuna tipologia (e, tra l'altro, **ripetuta** ad ogni nuovo assunto, che sia lavoratore temporaneo, a incarico o a tempo indeterminato).

Per questo noi proponiamo un altro modello, gestibile a costi contenuti e, se correttamente utilizzato, decisamente molto efficace.

Il modello di formazione che proponiamo

La normativa privacy è estremamente farraginosa e schizofrenica (nel senso che le regole per gli enti pubblici sono molto diverse da quelle per i privati ed inoltre, in molti casi, da settore a settore). Di solito i manuali la trattano tutta insieme, creando enorme confusione nel lettore. La forza dei nostri manuali è che ognuno contiene solo le regole realmente in vigore per quel settore, evitando di appesantire il lettore con regole che non lo riguardano. Si guadagna così enormemente in chiarezza, brevità ed efficacia. Questo è possibile grazie al fatto che i nostri manuali non sono stampati, ma forniti in files che il cliente scarica da internet, apre con password e stampa (e fotocopia) nella quantità di copie che gli servono.

Una serie completa di dispense speciali:

- modulari, **cioè** costruite per capitoli componibili, in modo da creare un "vestito su misura" per ciascun addetto ma anche per Responsabili e Titolari
- specializzate, a seconda dell'appartenenza ad una delle 3 categorie fondamentali: "Enti pubblici", "Privati ed Enti Pubblici Economici", "Sanità Pubblica e Privata" **(l**e dispense sono diverse a seconda del settore cui sono destinate, in modo da non creare confusioni, visto che le regole per questi settori sono parzialmente diverse**)**
- **differenziate a seconda dei livelli** dei destinatari **benché** complete per le esigenze di ciascun livello
- riproducibili in quantità illimitata purché all'interno dell'Azienda/Ente **(sarà ceduto il diritto di copyright)**
- **di facile comprensione perché** scritte da esperti in divulgazione che hanno tradotto in linguaggio comprensibile testi anche molto complessi, problematici ed approfonditi
- **molto economiche**, **grazie al fatto che** i nostri costi editoriali sono stati ridotti al minimo in quanto le dispense sono scaricabili tramite Internet e protette da una password che Vi sarà comunicata, poi saranno fotocopiate a Vs cura.
- costituenti **un corpus autosufficiente** per rispondere, in modo articolato ed esaustivo, grazie alla modularità, a qualsiasi esigenza formativa richiesta nel 99% dei casi
- ideali per il lavoro di gruppo, **sia leggendole insieme o dopo una lettura individuale come base da discutere successivamente insieme al Responsabile in riunioni di cui riterrà un sintetico verbale**

- **integrative di corsi tradizionali,** perché si possono utilizzare solo i moduli che completano e approfondiscono; **inoltre** offrono un percorso formativo completo agli addetti che per qualsiasi ragione non possono seguire i corsi **(assenze, indisponibilità del corso per tutti gli addetti, nuovi assunti)**
- **autodocumentanti la formazione**, poiché ogni dispensa si conclude con una scheda da riconsegnare al Titolare recante una dichiarazione di aver ricevuto e letto quello specifico materiale e, in alcuni casi, con dei quiz che l'addetto deve risolvere (cosicché conservando tutte le schede, si documenta per ciascuno il percorso formativo: nessun addetto potrà affermare di non essere stato messo in grado di affrontare adeguatamente i propri compiti).

Grazie alla modularità sarà possibile costruire facilmente quel **programma formativo analitico** che va obbligatoriamente inserito nel Documento Programmatico sulla Sicurezza (DPS).

Sottolineiamo che le dispense sono molto adatte come base:

- di un eventuale **lavoro di gruppo omogeneo** (leggendole insieme, discutendone sotto la guida di un Responsabile ed evidenziando i nodi più utili rispetto alle esigenze specifiche dell'Azienda/Ente o del reparto; utili anche esercitazioni applicative),
- di eventuali **brevi riunioni** successive alla lettura individuale (in cui si discutono questioni sollevate dai singoli sotto la guida di un Responsabile, sempre con un occhio alle esatte esigenze dell'Azienda/Ente o del reparto e all'opportunità di sviluppare esempi concreti).

In entrambi i casi, queste riunioni possono essere inserite nel programma formativo. Il verbale sintetico di queste riunioni recante i nomi dei partecipanti, insieme alle schede di attestazione individuale, sarà conservato in apposito fascicolo allegato al DPS, che documenterà i percorsi formativi di ciascun addetto.

Peraltro si può anche eventualmente rinunciare alle riunioni e contare sullo studio individuale, certificato dalla scheda di autovalutazione.

Come costruire un programma formativo adeguato

Primo passo

Si deve partire da una ricognizione di **TUTTE** le figure che hanno ricevuto una nomina a Incaricato o a Responsabile di trattamento (Impiegati, Tecnici, Collaboratori, Operai, Docenti, Esterni eletti in Organi Collegiali, etc.) oppure che dovranno occuparsi **anche** di eventuali funzioni speciali**, quali:**

- amministratore di sistema informatico
- addetto al backup periodico dei dati
- addetto all'aggiornamento periodico dell'antivirus e delle "patches" che aggiornano il sistema operativo o i programmi utilizzati
- addetto alle prove di ripristino su computer diverso in caso di disastro del computer normalmente utilizzato
- addetto alla custodia delle password (consegnate in busta chiusa da ciascun

Incaricato ad ogni rinnovo periodico) e della periodica ricognizione che alla scadenza tutti abbiano rinnovato la password

- addetto alla custodia della chiave degli archivi ad accesso selezionato o controllato e degli eventuali registri

Questo elenco, in realtà, dovrebbe esistere già ed essere obbligatoriamente inserito nel DPS come "Mansionario Privacy". Se non è ancora stato fatto, è l'occasione per occuparsene.

Secondo passo

Il passo successivo è raggruppare, laddove possibile, gli addetti per gruppi omogenei rispetto alle operazioni fondamentali da compiere in materia privacy (però è possibile che qualche addetto costituisca gruppo a se stante). Si otterrà così una lista di gruppi omogenei di addetti; i componenti di ciascun gruppo avranno identiche esigenze formative.

Se qualcuno di questi addetti ha funzioni aggiuntive o particolari, il suo nome va ripetuto creando un nuovo gruppo (di cui potrebbe rivelarsi anche l'unico componente), che ha ulteriori, specializzate, esigenze formative.

Terzo passo

A questo punto, a ogni gruppo si dovranno associare:

- **Un modulo formativo generale del livello di approfondimento richiesto**: "livello base" (compendio breve ed essenziale adatto a chi non ha impegni rilevanti nell'applicazione della normativa privacy) oppure "livello avanzato" (compendio più completo ed approfondito, adatto a chi svolge lavoro impiegatizio o front-office rispetto all'utenza oppure utilizza il computer o ricopre mansioni speciali). Di questo opuscolo va data una copia a ciascun addetto.
- **Tutte le schede tematiche necessarie per soddisfare le esigenze di formazione caratteristiche del gruppo**. In questo caso possono essere riprodotte in numero limitato ed essere prestate temporaneamente a ciascuno. Resteranno anche come biblioteca consultabile. Tutte insieme costituiscono un grosso manuale divulgativo. Ogni scheda (ovvero ogni nome di file) è connotato da un numero progressivo, per cui è facile individuarle senza equivoci e gestirle.

Un parola a parte va spesa sulla dispensa tematica "08) STRUMENTI DI ANALISI (O ESERCIZIARIO) PER CLASSIFICARE TRATTAMENTI E DATI, NONCHÉ PER VERIFICARE IL RISPETTO DI TUTTE LE REGOLE".

Si tratta di un formidabile strumento operativo per censire i trattamenti e i dati, classificarli e **verificare che tutte le regole siano rispettate.** E' costituito da 4 schede-tipo da compilare. Può essere utilizzato per un lavoro di schedatura totale delle attività della scuola in campo privacy, con la programmazione delle regole da applicare ai vari casi, costruendo uno strumentario applicativo e procedurale che guiderà il lavoro di tutti.

Se questo è già stato eseguito, in ogni caso queste schede possono servire per scopo didattico come esercitazione su casi concreti per far acquisire esperienza maggiore all'Incaricato.

Quarto passo

Dare disposizioni perché i nuovi arrivati (supplenti a termine o persone di ruolo) ricevano la serie di materiali necessaria appena arrivano. Il consiglio è di mettere nella copia della nomina che verrà loro data anche una menzione del "Kit Formazione" e la ricevuta per lo stesso.

Quinto passo

La documentazione dell'attività formativa.

Ogni opuscolo o scheda si conclude con un modulo già predisposto che il lettore deve completare, sottoscrivere e riconsegnare. Il "compendio" contiene anche una serie di facili domande in modalità quiz, che possono servire a verificare se la lettura è stata attenta e possono inoltre essere la base per eventuali riunioni chiarificatrici.

E' fondamentale che tutte le schede siano riconsegnate e poi conservate insieme al Documento programmatico per la Sicurezza, a dimostrazione dell'avvenuta esecuzione di questa specifica misura di sicurezza.

Cos'è il KIT FORMAZIONE

Il kit di formazione proposto è **riservato agli enti pubblici non economici** (in particolare la scuola), esclusi settori speciali e sanità (per quest'ultima è previsto un kit specifico). Per i privati (comprese le scuole private) e gli enti pubblici economici esiste un diverso kit, specifico per loro.

Il programma di formazione va integrato con l'illustrazione delle dotazioni di sicurezza effettivamente presenti nell'Ente e delle modalità d'uso delle stesse, nonché delle altre specificità dell'Ente dal punto di vista Privacy.

AVVERTENZA IMPORTANTE: questo materiale è destinato alla formazione, quindi può avere semplificazioni didattiche; pertanto non può essere utilizzato come manuale operativo per le questioni di rilevante complessità o importanza, PER LE QUALI VANNO CONSULTATI TESTI SPECIALISTICI.

➢ **ELENCO DI TUTTI I FILES CHE COMPONGONO IL "KIT FORMAZIONE PRIVACY"**

	Pag.	
I primi 2 files sono dedicati al Titolare/Responsabile Privacy e vanno letti per primi, per comprendere la struttura del "Kit Formazione Privacy" e come va utilizzato.		
01) LEGGIMI PER PRIMO	3	E' un file introduttivo, metodologico..
02) ISTRUZIONI PER LA FORMAZIONE	5	Illustrazione dei doveri del Titolare in materia di formazione. Seguono istruzioni pratiche su come soddisfare gli adempimenti utilizzando il nostro Kit.
I prossimi 2 files contengono i manuali generali, differenziati per livello di approfondimento. Ogni incaricato dovrebbe ricevere copia dell'uno o dell'altro. Presentano alla fine un modulo di ricevuta da conservare come prova dell'avvenuta formazione, che reca anche dei quiz cui rispondere.		
03) COMPENDIO LIVELLO BASE	25	Tutti i principali aspetti della normativa Privacy illustrati in modo chiaro per Incaricati con compiti di limitata responsabilità in materia Privacy. Soddisfa tutti i requisiti formativi di legge (25 pagine).
04) COMPENDIO LIVELLO AVANZATO	41	Sintesi ragionata di tutta la principale normativa Privacy per Incaricati con compiti di qualche responsabilità nella gestione dei

		trattamenti (41 pagine).
Tutti i files che seguono costituiscono una sorta di biblioteca di schede tematiche di approfondimento che gli Incaricati possono consultare in relazione agli argomenti di cui si occupano. Al bisogno certe schede possono essere riprodotte per darne copia a Incaricati. Presentano anch'esse alla fine un modulo di ricevuta da conservare come prova dell'avvenuta formazione. Si segnala, in particolare, la scheda n° 8, che è sia un prezioso strumento di lavoro, sia un eventuale eserciziario per gli Incaricati che hanno i compiti più delicati.		
05) INFORMATIVA – APPROFONDIMENTI	19	Approfondimento indispensabile per ogni Incaricato che raccoglie dati (sportello, protocollo, ecc.).
06) CENSIMENTO DEI TRATTAMENTI	7	Insegna a distinguere un trattamento da un altro.
07) CLASSIFICAZIONE DEI DATI	13	Insegna a classificare i dati personali in base alle note categorie: dati comuni, particolari, sensibili e giudiziari.
08) STRUMENTI DI ANALISI (O ESERCIZIARIO) PER CLASSIFICARE TRATTAMENTI E DATI, NONCHÉ PER VERIFICARE IL RISPETTO DI TUTTE LE REGOLE	7	Un formidabile strumento operativo per censire i trattamenti ed i dati, classificarli e verificare che tutte le regole siano rispettate. E' costituito da 4 schede-tipo da compilare. E' anche un ottimo strumento per esercitarsi acquisendo esperienza operativa. Consigliato a tutti gli Incaricati che hanno compiti di qualche responsabilità.
09) REGOLE DEL TRATTAMENTO	23	Approfondimento sulle regole del trattamento di dati.
10) QUANDO E' LECITO TRATTARE DATI	11	Approfondimento sui presupposti di legittimità del trattamento di dati personali, escluse comunicazione e diffusione.
11) QUANDO E' LECITO COMUNICARE DATI	20	Approfondimento sui presupposti di legittimità della comunicazione di dati.
12) QUANDO E' LECITO DIFFONDERE DATI	24	Approfondimento sui presupposti di legittimità della diffusione di dati.
13) GESTIONE DIPENDENTI	26	Consigli per la gestione dei dipendenti.
14) GESTIONE CLIENTI-FORNITORI	14	Consigli per la gestione dei clienti e fornitori .
15) GESTIONE PROTOCOLLO E SPORTELLO	3	Consigli per le procedure di raccolta dei dati e per le operazioni di spedizione degli stessi.
16) DIRITTI DELL'INTERESSATO E DI CHIUNQUE	22	Approfondimento sui diritti dell'Interessato e del meno noto diritto di chiunque ad avere informazioni su qualsiasi Titolare.
17) ACCESSO DI TERZI AI DATI	5	Approfondimento sulla Legge 241.
18) SICUREZZA STRUMENTI ELETTRONICI	14	Panoramica approfondita delle misure di sicurezza per i computers.
19) SICUREZZA DOCUMENTI	10	Panoramica delle misure di sicurezza per la

CARTACEI.		gestione dei documenti cartacei.
20) PASSWORD E COME INVENTARLE	6	Come gestire le password e consigli pratici per creare password facilmente ricordabili e su come modificarle per riutilizzarle nel tempo.
21) ANTIVIRUS E FIREWALL	5	Spiegazione della normativa e istruzioni per applicarla; consigli utili operativi.
22) BACKUP E RIPRISTINO DATI	11	Spiegazione delle procedure necessarie per applicare la normativa: realizzazione copie di salvataggio, ripristino dei dati, predisposizione del piano obbligatorio di 'disaster recovery' e … vari consigli pratici sulle opportunità offerte dalla tecnologia e dal software.
23) AGGIORNAMENTO ANTIVIRUS, FIREWALL E PROGRAMMI	2	Spiegazione della normativa e delle tecniche per attuare l'aggiornamento obbligatorio dei programmi.
24) CIFRATURA OBBLIGATORIA DEI DATI SENSIBILI E GIUDIZIARI TRATTATI CON IL COMPUTER	2	Illustra una misura di sicurezza poco nota e di solito male interpretata, obbligatoria per tutti gli Enti Pubblici, dando consigli utili per conformarsi alle norme sulla cifratura obbligatoria dei dati sensibili e giudiziari trattati con il computer.
25) PROFILI SANZIONATORI	14	Un quadro completo delle sanzioni amministrative, penali, civili e contabili legate al D. Lgs. 196.
26) GESTIONE DOCUMENTI A FINE TRATTAMENTO	2	Approfondimento delle normative in materia di conservazione/distruzione dei documenti.
27) DLGS 196 AGGIORNATO	55	Testo completo, compreso Allegato B, nella versione aggiornata dopo le modifiche fino a luglio 2005.
28) AUTORIZZAZIONI GENERALI	38	Il testo completo reso chiaro.
29) LA VIDEOSORVEGLIANZA	4	Breve quadro delle regole
30) SANITÀ	3	Breve panoramica sulle regole speciali per il settore sanità, anche dal punto di vista dei diritti del paziente.
31) TELEFONIA	2	I diritti dell'utente di servizi di telefonia fissa/mobile.
32) SCUOLA PUBBLICA	10	Breve approfondimento sul tema della scuola pubblica. Contiene anche il provvedimento del Garante del 26.07.05 su Portfolio e valutazioni.

Nota prot. n. 7657 del 20.12.2005

Nota prot. n. 7657 del 20.12.2005
Genitori separati non conviventi. Richiesta documentazione carriera scolastica dei figli

Con la **nota prot. n. 7657 del 20 dicembre 2005** avente per oggetto *"Genitori separati non conviventi. Richiesta documentazione carriera scolastica dei figli"* il MIUR

1. ✓ *invita* gli uffici periferici della propria amministrazione - *a* seguito del parere di merito del Ministero della Giustizia, relativo alla possibilità per il genitore non affidatario, in situazione di separazione e/o divorzio, di potere esercitare il diritto di seguire il figlio nel percorso scolastico - a tener conto:
    1. • che la potestà attribuita ad entrambi i genitori deve essere esercitata di comune accordo (art. 316 codice civile) o quantomeno concordata nelle linee generali di indirizzo, sulla base delle quali ciascun genitore potrà e dovrà operare anche separatamente
    2. • che anche quando l'esercizio della potestà è attribuito ad uno solo dei genitori, in genere il genitore affidatario, le decisioni di maggiore interesse sono adottate da entrambi i coniugi (art. 155 c.c.)
    3. • che il coniuge, cui i figli non siano affidati, ha il diritto e il dovere di vigilare sulla loro istruzione ed educazione
    4. • che si può, altresì, affermare che la funzione educativa - di cui peraltro la potestà è mero strumento - deve svolgersi tenendo conto in via ria della necessità di sviluppo della personalità del figlio, inteso come soggetto di diritti nella sua centralità, anziché delle aspettative e degli interessi personali dei genitori
    5. • che è proprio su tali comportamenti, quando si configurino gravi forme di carenza di assistenza e cura ovvero abuso, che il genitore, affidatario o non affidatario, potrà incorrere nella decadenza della potestà genitoriale su provvedimento del giudice ai sensi degli artt. 330 e seguenti c.c.

6. • che solo in tal caso, a tutela del figlio nei confronti del quale è stata posta in essere la condotta pregiudizievole, il genitore decaduto dalla potestà sarà conseguentemente decaduto da qualunque diritto dovere nei confronti dell'educazione dei figli

2. ✓ sollecita i medesimi uffici a voler favorire l'esercizio del diritto-dovere del genitore separato o divorziato non affidatario (articoli 155 e 317 c.c.) di vigilare sull'istruzione ed educazione dei figli e conseguentemente di accedere alla documentazione scolastica degli stessi.

4. Misure Minime di Sicurezza: schemi riepilogativi.

PRINCIPALI MISURE MINIME DI SICUREZZA
CONTENUTE NEL DISCIPLINARE TECNICO (All. B)
AL CODICE DELLA PRIVACY

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI			
MISURA DI SICUREZZA	**DESCRIZIONE E/O ESEMPIO**	**AGGIORNAMENTO**	**NORMA (Alleg. B)**
Redazione di istruzioni scritte agli incaricati	Redazione di istruzioni scritte finalizzate al controllo e alla custodia dei documenti contenenti dati personali	Periodico (almeno annuale)	Per maggiori dettagli si rinvia alle disposizioni da n.27 a n. 28
Sistema di accesso selezionato e controllato agli archivi	L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato. In mancanza di strumenti elettronici per il controllo degli accessi o di incaricati alla vigilanza le persone che vi accedono devono essere preventivamente autorizzate.	"…"	Per maggiori dettagli si rinvia alla disposizione n.29

TRATTAMENTI CON STRUMENTI ELETTRONICI			
MISURA DI SICUREZZA	**DESCRIZIONE E/O ESEMPIO**	**AGGIORNAMENTO E NOTE**	**NORME (Alleg. B)**
Sistema di Autenticazione Informatica	*User-ID e Password*	Periodico (*almeno annuale*) N.B.: in caso di trattamento di dati sensibili e giudiziari la password deve essere modificata ogni 3 mesi	Per maggiori dettagli si rinvia alle disposizioni da n.1 a n. 11 e n. 15
Sistema di autorizzazione	Creazione e gestione di diversi profili "utente" con poteri di accesso/modifica ai dati e ai programmi differenziati in base alle effettive mansioni e responsabilità assegnate	Periodico (*almeno annuale*)	Per maggiori dettagli si rinvia alle disposizioni da n.12 a n.14
Sistema di protezione contro i software dannosi ai sensi dell'art. 615 quinquies c.p. (*virus, worm, trojan horse…*)	Antivirus e altri strumenti elettronici (software e/o hardware) tesi ad impedire l'infezione e la diffusione di programmi dannosi.	Periodico (*almeno semestrale*)	Per maggiori dettagli si rinvia alla disposizione n. 16
Sistema di protezione contro accessi abusivi (art. 615 ter c.p.)	Firewall ed altri strumenti elettronici (software e/o hardware) tesi ad impedire l'accesso abusivo ai dati sensibili e giudiziari (in quest'ampia definizione rientrano in astratto anche i sistemi "Intrusion Detection Sstems")	Periodico (*almeno semestrale*)	Per maggiori dettagli si rinvia alle disposizioni da n. 20
Sistema di aggiornamento periodico dei programmi volti a prevenire le vulnerabilità	I software utilizzati (dal sistema operativo ai vari software applicativi) devono essere costantemente aggiornati per eliminarne le vulnerabilità.	Periodico (*almeno annuale*) N.B.: in caso di trattamento di dati sensibili e giudiziari l'aggiornamento deve essere almeno semestrale	Per maggiori dettagli si rinvia alla disposizione n. 17
Sistema di back up	Salvataggio (copia) dei dati su supporti di sicurezza.	Periodico (*almeno settimanale*)	Per maggiori dettagli si rinvia alla disposizione n. 18
Disaster Recovery	*Adozione di misure idonee per il ripristino della disponibilità dei dati sensibili o giudiziari in seguito a distruzione o danneggiamento.*	N.B.: l'accesso ai dati deve essere ripristinato entro e non oltre 7 gg.	Per maggiori dettagli si rinvia alle disposizioni da n.21 a 23
Documento Programmatico Sulla Sicurezza	Redazione di un documento organico che, partendo da un'attenta analisi dei rischi del sistema, metta in risalto le contromisure tecniche e procedurali idonee a prevenirli e contenerli.	Periodico (entro il 31 marzo di ogni anno)	Per maggiori dettagli si rinvia alle disposizioni da n. 19 a n. 19.8