



Codice sulla Privacy

Decreto Legge 196/2003

Istituto Caterina Caniana - Bergamo

Premessa

Il Decreto Legge 196/2003 è entrato in vigore il 01/01/2004 ed ha raccolto in un unico testo le precedenti leggi, decreti e codici deontologici in tema di Privacy.

Obiettivo

Tutte le aziende trattano i dati personali in conformità del Codice stesso, agendo su 3 fronti:

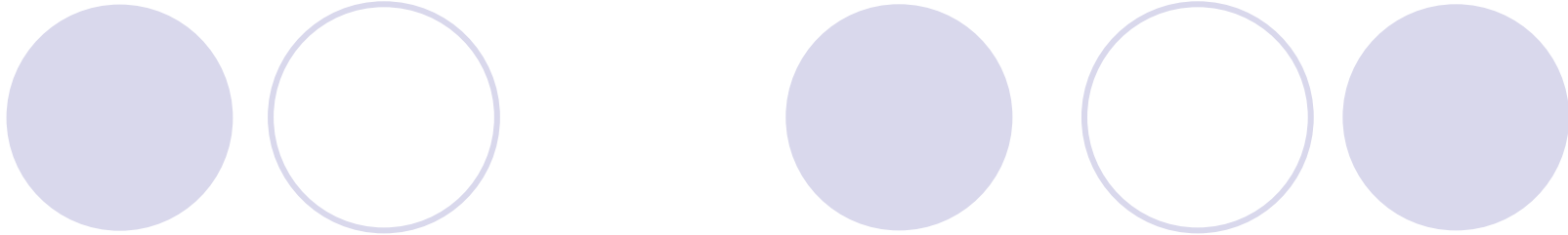
- pianificazione delle misure organizzative, amministrative e tecniche di sicurezza attraverso un documento formale denominato Documento Programmatico sulla Sicurezza (DPS).**
- adeguamento alle misure tecniche minime di sicurezza definite nell'allegato B del D.Lgs 196/2003**
- fornitura di un'informativa trasparente e completa dei trattamenti dei dati personali ai relativi interessati ed ottenimento del consenso (se e quando necessario)**



Documento Programmatico sulla Sicurezza

Contenuti:

- **soggetti coinvolti nel trattamento dei dati (titolare, responsabili e incaricati)**
- **formazione del personale in materia di sicurezza**
- **descrizione delle procedure di autenticazione del soggetto per l'accesso ai dati, attraverso sistemi basati su password, firma digitale, dispositivi biometrici di riconoscimento**
- **sistema informativo, basi di dati, hardware e software utilizzati in azienda**
- **politiche di backup, copie di sicurezza dei dati**
- **rischi relativi al trattamento dei dati sensibili eventualmente trattati, contromisure adottate in caso di disastri (disaster recovery)**



Attività

- **nomina del titolare trattamento dati**
- **nomina di uno o più responsabili del trattamento dati**
- **nomina degli addetti al trattamento dati**
- **stesura del Documento Programmatico sulla Sicurezza**

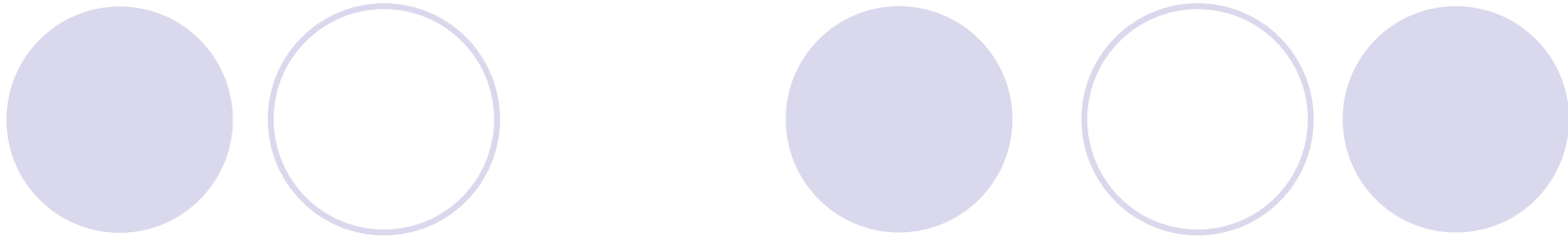
Scadenza

Il Documento Programmatico sulla Sicurezza deve essere redatto entro il 30/06/2005 e dovrà essere aggiornato ogni anno entro il 31 marzo. Le aziende che hanno l'obbligo di pubblicazione del bilancio devono dichiarare nella lettera accompagnatoria al bilancio che il Documento Programmatico sulla Sicurezza è stato redatto.



Termini e definizioni

- ❑ **Dati personali:** qualunque informazione relativa a persona fisica, giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi informazione, ivi compreso un numero di identificazione personale
- ❑ **Dati sensibili:** dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai 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.
- ❑ **Dati giudiziari:** 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 DPR 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 ai sensi degli articoli 60 e 61 del codice di procedura penale.
- ❑ **Autenticazione:** processo informatico di riconoscimento dell'utente, nel momento in cui richiede l'accesso al sistema informativo.
- ❑ **Firewall:** dispositivo di filtro dei dati, programmato per regolare il traffico e prevenire intrusioni alla rete dall'esterno



- ❑ **Titolare del trattamento:** è la persona o l'Ente decisionale nell'azienda che riveste compiti manageriali e decisionali, anche in materia di sicurezza.
- ❑ **Responsabili del trattamento:** il Titolare può nominare uno o più Responsabili del Trattamento, che per idoneità e competenza ha il potere esecutivo di organizzare la politica di sicurezza dei dati sensibili per la privacy.
- ❑ **Incaricati:** sono le persone che trattano i dati sensibili all'interno del sistema informativo.

Procedure:

• **Sistemi di autenticazione per l'accesso ai dati:** l'autenticazione è effettuata genericamente tramite inserimento di un nome utente e password, una parola chiave la cui custodia e segretezza è responsabilità dell'utente stesso. Le pwd devono essere abbastanza lunghe, bisogna usare utilizzare parole chiave non di uso comune, avere una scadenza prefissata ed essere cambiate di frequente.

• **Sistema informativo ⇒ server ad accesso pubblico e portali Web:** è bene evitare la pubblicazione sul sito web aperto al pubblico di dati classificati come sensibili per la privacy

• **Sistema informativo ⇒ rete aziendale, hardware di rete e personal computer:** il DPS richiede un elenco dell'hardware utilizzato nel trattamento delle informazioni, ossia:

- ✓ elaboratori elettronici utilizzati in azienda come client
- ✓ server installati sulla rete, con elenco dei servizi offerti
- ✓ dispositivi di rete, hub, switch, router per lo smistamento dei dati
- ✓ connessioni in rete locale LAN e rete geografica WAN
- ✓ Postazioni mobili di lavoro
- ✓ dispositivi hardware a difesa da intrusioni esterne e politica di gestione dei rischi per l'integrità dei dati derivanti da furti o eventi/calamità naturali
- ✓ dispositivi di backup dei dati e relativa politica

Dati trattati dai docenti

- **Il registro personale**
- **Il registro di sezione/classe**
- **Il registro dei verbali del consiglio di intersezione/interclasse**
- **La documentazione relativa alla programmazione didattica**
- **I documenti di valutazione**
- **Gli elaborati**
- **I certificati medici degli allievi**
- **La corrispondenza con le famiglie**
- **I dati personali devono essere conservati in contenitori adeguati (schedari, armadi) dotati di serratura efficiente e sicura.**
- **I dati idonei a rivelare lo stato di salute degli alunni, trattati esclusivamente per finalità previste dalla legge, vanno conservati separatamente da altri dati personali.**
- **Tali dati consistono essenzialmente in certificati medici consegnati dagli alunni o dai genitori ai docenti per scopi definiti da norme di legge (giustificazione assenze, esonero da attività di educazione fisica, necessità di particolari diete alimentari ecc).**
- **Dopo la ricezione i dati vanno custoditi in appositi contenitori chiusi.**
- **I certificati riguardanti la necessità di particolari diete alimentari potranno, in caso di necessità, essere comunicati al soggetto che espleta il servizio mensa, previa nomina a responsabile esterno del trattamento da parte del titolare.**

Dati trattati dal personale amministrativo

- **Le banche dati su supporto cartaceo e/o informatizzato, contenenti dati personali, alle quali ha accesso il personale di segreteria sono:**
- **fascicoli relativi al personale della scuola**
- **fascicoli degli alunni ed ex alunni**
- **anagrafe fornitori, contratti**
- **documentazione finanziaria e contabile**
- **registro degli infortuni**
- **Il trattamento dei dati di pertinenza esclusiva del personale ATA viene effettuato con strumenti elettronici e non.**
- **I dati personali devono essere conservati in contenitori adeguati (schedari, armadi) dotati di serratura efficiente e sicura.**
- **I dati idonei a rivelare lo stato di salute del personale, docente ed ATA, e degli alunni viene trattato esclusivamente per finalità previste dalla legge.**
- **Secondo quanto prescritto dall'articolo 22 comma 7 del D. L. vo 196/2003 i dati idonei a rivelare lo stato di salute vanno conservati separatamente da altri dati personali; inoltre il comma 7 dello stesso articolo dispone che i dati idonei a rivelare lo stato di salute, qualora contenuti in banche dati informatiche vengano trattati "con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altre soluzioni, che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità".**

Dati trattati dal personale amministrativo

- Riguardo al trattamento senza l'ausilio di strumenti elettronici, dei dati di cui si tratta si stabilisce quanto segue:
 - a) **Dati riguardanti il personale docente ed ATA**
 - I dati consistono essenzialmente in certificati medici consegnati o fatti pervenire all'ufficio di segreteria.
 - Dopo la ricezione, durante il trattamento (protocollo etc) saranno inseriti in un contenitore chiuso riferito all'interessato e successivamente inseriti nel fascicolo personale, dove saranno conservati all'interno di una busta chiusa recante l'indicazione del contenuto separatamente dagli altri documenti.
 - b) **Dati riguardanti gli alunni**
 - I dati consistono essenzialmente in certificati medici consegnati dagli alunni o dai genitori ai docenti o al personale ATA, per scopi definiti da norme di legge (giustificazione assenze; esonero da attività di educazione fisica, necessità di particolari diete alimentari etc.)
 - Dopo la ricezione i dati saranno inseriti in un contenitore chiuso riferito all'interessato e successivamente trattati da personale incaricato e custoditi in appositi contenitori chiusi.
 - I certificati riguardanti la necessità di particolari diete alimentari, potranno in caso di necessità, essere comunicati al soggetto che espleta il servizio mensa previamente nominato responsabile esterno del trattamento da parte del titolare.