



**D. Lgs. 30 giugno  
2003, n. 196**



**Codice in materia di protezione  
dei dati personali**

## Definizioni

- Dato personale: qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4, comma 1, lett. B))





## Definizioni

- Esempio: nome, cognome, telefono, fax, codice fiscale, patente, partita IVA, immagini, fotografie, dati bancari, ecc)



## Definizioni

- **Dati sensibili:** i dati personali idonei a rilevare l'origine razziale/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 rilevare lo stato di salute e la vita sessuale (art. 4, comma 1, lett. d))



## Definizioni

- Esempio: razza, etnia, ideologia politica (ritenute sindacali), religione (contributo 8 per mille), certificati di malattia, certificati di infortunio, prescrizioni mediche, radiografie, ecc.

# Definizioni

- Dati giudiziari: i dati personali a rilevare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14.11.2002, 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. (art. 4, comma 1, lett. e))





## Definizioni

- Esempio: provvedimenti amministrativi o penali, la qualità di indagato o di imputato, ecc)

# Definizioni

- **Trattamento:**... operazioni effettuate, anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione di dati, anche se non registrati in una banca dati.





# Soggetti

- Dipendenti;
- Fornitori;
- Clienti;
- Utenti;
- Soci;
- Pazienti;
- Colleghi.

# Attività preliminari

- 1) Inventariare i dati oggetto di trattamento (dati personali, dati sensibili, dati giudiziari);
- 2) Adottare misure di sicurezza minime che proteggano i dati dalla distruzione o perdita anche accidentale, dal trattamento non autorizzato o non conforme alle finalità per cui sono stati raccolti, ecc (password, antivirus, installazione di porta antincendio a protezione del server, custodia in luogo segreto delle copie di back up, ecc);
- 3) Individuare i soggetti che hanno accesso ai dati (titolare del trattamento, resp.le del trattamento, incaricati al trattamento, preposto alla custodia della parola chiave, ecc).
- 4) Informativa (art. 13) ai soggetti.





## Sicurezza dei dati e dei sistemi

- ✓ Trattamenti dei dati personali senza l'ausilio di strumenti elettronici
- ✓ Trattamenti dei dati personali con strumenti elettronici



# Trattamenti dei dati personali senza l'ausilio di strumenti elettronici

Il trattamento è consentito solo se:

- Sono adottate le misure minime di sicurezza individuate dal codice (art. 35);
- Le misure minime di sicurezza sono adottate con le modalità previste dal disciplinare tecnico (allegato B).
- Esempio:
  - ✓ Ambito e responsabilità di trattamento;
  - ✓ Procedure di archiviazione;
  - ✓ Procedure di utilizzo dei documenti;
  - ✓ Modalità di accesso agli archivi.

# Trattamenti dei dati personali con l'ausilio di strumenti elettronici

Il trattamento è consentito solo se sono adottati:

- Sistemi di autenticazione;
- Sistemi di autorizzazione;
- Sistemi di back up;
- Protezione degli strumenti elettronici;
- Procedure di ripristino dei dati;
- Sistemi di cifratura o codici identificativi per determinati trattamenti di dati idonei a rilevare lo stato di salute o la vita sessuale effettuati da organismi sanitari;
- Ecc.





## Trattamenti dei dati sensibili e giudiziari con l'ausilio di strumenti elettronici

- Predisposizione del Documento Programmatico sulla Sicurezza (DPS)



## Aggiornamento software

- Aggiornamento periodico del software regolarmente licenziato
- Windows 95/98 e ME non sono più a norma minima di sicurezza



## Aggiornamento hardware

- Le nuove disposizioni chiedono un aggiornamento tecnologico
- I nuovi sistemi operativi hanno bisogno di adeguate risorse hardware

## Le scadenze



Entrata in vigore	01.01.2004
DPS	30.06.2004
Notificazione	30.04.2004
Misure minime	30.06.2004
Adeguamento tecnologico	31.12.2004

# Notificazione del trattamento al garante

- Solo per i casi indicati dal codice (art. 37)
- Estratto
  - Dati genetici, biometrici;
  - Dati che indicano la posizione geografica di persone od oggetti;
  - Dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
  - Dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
  - Dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti ;
  - Dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
  - Dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.



# Sanzioni

Il mancato rispetto delle norme dettate dal “Codice sulla privacy“ espone al rischio di gravi sanzioni:

- Reclusione;
- Pena pecuniaria fino a 124.000 euro;
- Risarcimento dei danni all’interessato ai sensi dell’art. 2050 del Cod. Civ..



# Documento programmatico sulla sicurezza - Autovalutazione



Elemento 196/2003	SI	NO
Elenco dei trattamenti di dati personali		
Distribuzione dei compiti e responsabilità		
Analisi dei rischi sui dati		
Misure da adottare per garantire integrità disponibilità dei dati, protezione aree, locali		
Descrizione dei criteri e modalità per il ripristino dei dati in seguito a distruzione o danneggiamento		
Interventi formativi degli incaricati al trattamento		
Descrizione criteri da adottare per garantire l'adozione di misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura		
Per i dati personali idonei a rilevare lo stato di salute e la vita sessuale sono stati individuati criteri di cifratura o separazione di tali dati dagli altri personali dell'interessato		

# Documento programmatico sulla sicurezza - Autovalutazione

Elemento 196/2003	SI	NO
Dati sensibili o giudiziari sono protetti contro l'accesso abusivo mediante idonei strumenti elettronici		
Idonee istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti		
I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ove possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelleggibili e tecnicamente in alcun modo ricostruibili		
Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni		
Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare		



# Documento programmatico sulla sicurezza - Autovalutazione



Elemento 196/2003	SI	NO
Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico del presente disciplinare		

# Trattamenti senza l'ausilio di strumenti elettronici - Autovalutazione



Elemento 196/2003	SI	NO
<p>Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.</p>		
<p>Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.</p>		
<p>L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.</p>		

# Trattamenti senza l'ausilio di strumenti elettronici - Autovalutazione



Elemento 196/2003	SI	NO
Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.		



- La presentazione non è né esaustiva né sostitutiva rispetto al testo del Decreto Legislativo cui, comunque, si rimanda ai fini di una conoscenza completa della disciplina vigente in materia di trattamento di dati personali