



CODICE DELLA PRIVACY

Dlgs. 196/2003

- Guida per gli odontotecnici

DEFINIZIONI ESSENZIALI

TRATTAMENTO DATI

Qualunque operazione o complesso di operazioni effettuato anche senza l'ausilio di strumenti elettronici (es.: manualmente) concernente:

raccolta

registrazione

organizzazione

conservazione

elaborazione

modificazione

selezione

estrazione

raffronto

utilizzo

interconnessione

blocco

comunicazione

diffusione

cancellazione

distruzione

consultazione

prima non esplicitata ma desunta dalla definizione di comunicazione

BANCA DATI

Qualsiasi complesso organizzato di dati personali ripartito in una o più unità dislocate in uno o più siti



Dato personale

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

Dati esclusivamente personali (art. 5.3)

Le disposizioni del Codice non riguardano il trattamento di dati effettuato per fini esclusivamente personali sempre che non si abbia diffusione o comunicazione sistematica

Rimane la responsabilità per danni cagionati (15) e il dovere di rispettare gli **obblighi generali di sicurezza** (31)



Dati identificativi

Dati personali che permettono l'identificazione diretta dell'interessato

Dati sensibili

Dati idonei a rivelare

L'origine razziale ed etnica

Le convinzioni religiose, filosofiche e di altro genere

Le opinioni politiche

L'adesione a partiti, sindacati, associazioni od organizzazioni a carattere filosofico, politico o sindacale

Lo stato di salute e la vita sessuale



Dati giudiziari

Dati personali idonei a rivelare provvedimenti in materia di **casellario giudiziale** (*), di **anagrafe delle sanzioni amministrative dipendenti da reato** e • • **dei relativi carichi pendenti** (art. 3, c 1, lett a/o e r/u del D.P.R n. 313/2002), o la qualità di imputato o di indagato (ai sensi degli artt. 60/61 del C.P.P.)

(*). Con esclusione di quelli conoscibili:

- definitivi di interdizione, inabilitazione e quelli di revoca
- che dichiarano fallito l'imprenditore; di omologazione del concordato fallimentare; di chiusura del fallimento; di riabilitazione del fallito



Titolare del trattamento (art. 28)

È la persona fisica, giuridica, ente, associazione, P.A. cui compete la decisione sulle finalità, modalità e mezzi del trattamento e sugli strumenti utilizzati (ivi compreso il profilo della sicurezza)

Se il trattamento è effettuato da una persona giuridica, da una P.A. o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo

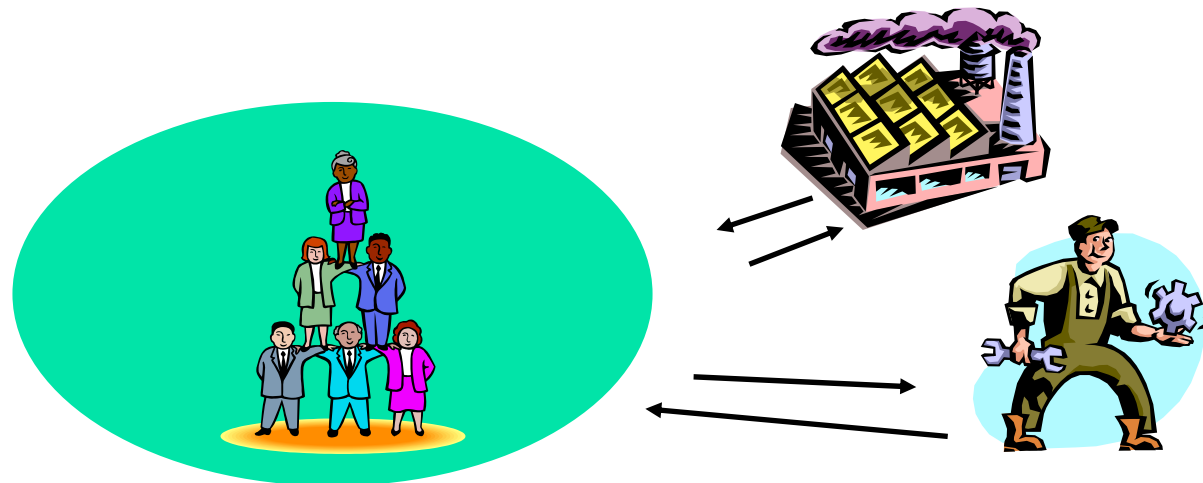
Responsabile del trattamento (art. 29)

È la persona fisica, giuridica, ente, P.A. ... preposta dal titolare del trattamento (art. 4.1 lett. g)

Incaricati del trattamento

Sono le persone fisiche che effettuano le operazioni del trattamento, attenendosi alle istruzioni impartite dal titolare o responsabile (art. 30, comma 1), che, per iscritto (comma 2), ha loro attribuito questo compito individuando puntualmente l'ambito del trattamento consentito

Inserendo o elaborando i dati a computer o attendendo all'archivio i dipendenti vengono a conoscenza dei dati personali



Informativa (art. 13)

Prima di effettuare il trattamento dei dati personali il titolare del trattamento ha **SEMPRE** l'obbligo di fornire succinta ma chiara informazione (ORALE O SCRITTA) circa:

> Le finalità della raccolta

Trattamento giuridico ed economico del personale

Gestione del personale

Adempimenti di obblighi fiscali e contabili

Gestione di fornitori

Gestione della clientela

Gestione del contenzioso

> Le modalità del trattamento

Manuale



Informatica



Telematica



> Natura facoltativa/obbligatoria del trattamento

> Le conseguenze di un rifiuto a rispondere

> I soggetti o le categorie di soggetti a cui i dati potranno essere comunicati **O CHE POSSONO VENIRNE A CONOSCENZA IN QUALITA' DI RESPONSABILI OD INCARICATI** (aggiunta preoccupante: difficoltà operative per mantenere un'informativa completa!) e l'**ambito di diffusione** dei dati

Si rischierebbe di dover informare sulla quasi totalità dell'organico e sulle variazioni ... vista anche la "definizione" di comunicazione si confida trattarsi di e

Se così non fosse, qual è la possibile formula utilizzabile?

• " ... essere comunicati a tutti gli incaricati della società"

• " ... essere comunicati a tutti gli incaricati:
Sig. Paolo Rossi; Sig.ra Maria Bianchi "

• " ... essere comunicati a tutti gli incaricati dell'ufficio
paghe, amministrazione, commerciale"

Troppo
banale

Troppo
dettaglio

Sembra
adeguato

> I diritti che il Codice attribuisce (art. 7) all'interessato

Come già detto: quale formula è sufficiente?

> Gli estremi identificativi:

- del TITOLARE

- del RESPONSABILE se designato

- del RAPPRESENTANTE in Italia del titolare extraeuropeo

- dell'eventuale RESPONSABILE DESIGNATO PER I RAPPORTI CON CHI ESERCITA I "DIRITTI DELL'INTERESSATO"

Se ci sono più responsabili

basta un solo nominativo

occorre però indicare:

sito in rete

altro modo agevole

per reperire l'elenco completo



Consenso (artt. 23/26)

Il trattamento dei dati personali da parte di privati/enti pubblici economici è ammesso solo col “consenso espresso” (non presunto, non implicito) dell’interessato, che può prestarlo **per una o più operazioni o per l’intero trattamento**

Il consenso deve essere **raccolto per iscritto** (sempre, per i dati sensibili) od anche **oralmente documentandolo per iscritto**

- **preceduto da chiara informativa** che gli permetta la decisione con nozione di causa



Casi di esclusione consenso in generale e salve le disposizioni per settori specifici (art.24)

Quando il trattamento:

- riguarda dati raccolti e detenuti in base ad un obbligo di legge, regolamento o normativa comunitaria
- è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere – prima della conclusione del contratto – “a specifiche richieste dell'interessato” (formula diversa da “misure precontrattuali adottate su sua richiesta”?)
- riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, nel rispetto delle norme che regolano la conoscibilità e pubblicità di tali dati (es.: elenco telefonico non serve all'esercizio del marketing)
- è finalizzato unicamente a scopi di ricerca storica o scientifica o di statistica e avviene nel rispetto dei rispettivi codici di deontologia

• riguarda dati relativi allo svolgimento di **attività economiche** (dell'interessato) nel rispetto della normativa sul segreto aziendale e industriale

• è necessario per indagini difensive ... o, comunque, per far valere o difendere un diritto in sede giudiziaria

LIMITI:

- per queste finalità

- per il periodo strettamente necessario a perseguirle

- nel rispetto della vigente normativa in materia di segreto aziendale e industriale

• è necessario, nei casi individuati dal Garante, per perseguire un legittimo interesse del titolare/o terzo destinatario dei dati e non prevalgono *diritti, libertà, dignità, interessi legittimi dell'interessato* – diffusione esclusa.

N.B. Significativo il riferimento esplicito all'attività dei “*gruppi bancari*” e delle “*società controllate o collegate*”

MISURE DI SICUREZZA

OBBLIGO GENERALE (art. 31)

I dati personali 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**
- **accesso non autorizzato**
- **trattamento non consentito**
- **trattamento non conforme alle finalità della raccolta**

Tenendo conto:

- **delle conoscenze acquisite in base al progresso tecnico**
- **della natura dei dati**
- **delle specifiche caratteristiche del trattamento**

LE MISURE MINIME DI SICUREZZA

Dal **PRINCIPIO DI NECESSITÀ** (art. 3) - ridurre al minimo l'utilizzo dei dati

All'**OBBLIGO GENERALE DI SICUREZZA** (art. 31) – derivante dallo svolgimento di un'attività valutata pericolosa, art. 15 → art. 2050 C.C. – con responsabilità civile oggettiva, patrimoniale e non patrimoniale

Alle **MISURE MINIME DI SICUREZZA** (art. 33/35)
Misure volte a garantire un “LIVELLO MINIMO DI PROTEZIONE”.
Prescrizioni specifiche del Codice, alle quali il titolare e responsabile debbono attenersi (sanzionate penalmente) individuate in un **DISCIPLINARE TECNICO**, allegato al CODICE

Il disciplinare viene aggiornato periodicamente (decreto del Ministro della giustizia di concerto col Ministro per le innovazioni e le tecnologie) in base all'evoluzione tecnica ed all'esperienza maturata nel settore (art. 36)

PER I TRATTAMENTI CON STRUMENTI ELETTRONICI (art. 34) **Misure minime (nei modi previsti dal disciplinare)**

- sistema di autenticazione informatica
- procedure di gestione delle credenziali di autenticazione
- sistema di autorizzazione
- aggiornamento periodico dell'ambito di trattamento consentito a incaricati/manutentori
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, accessi non consentiti e a determinati programmi informatici
- procedure: per la custodia di copie di sicurezza; per il ripristino della disponibilità dei dati e dei sistemi
- per gli organismi sanitari tecniche di cifratura o codici identificativi per trattamenti idonei a rivelare salute/vita sessuale
- documento programmatico sulla sicurezza aggiornato





Riepilogo per gli odontotecnici

Per gli obblighi previsti dalla Direttiva sui dispositivi medici, gli odontotecnici trattano correntemente dati sanitari e, conseguentemente, sono destinatari degli obblighi specifici previsti dal Codice della privacy al Titolo V^o, Capo I e II, articoli dal 75 all' 84.



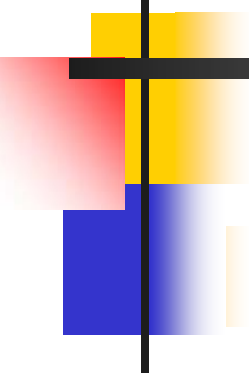
Adempimenti privacy odontotecnici

- In quanto esercenti di professione sanitaria, gli odontotecnici sono esentati dall'obbligo di comunicazione al Garante
- Non sono invece esentati dagli obblighi inerenti l'informativa/consenso dell'interessato al trattamento
- Conseguentemente, non potendo avere accesso diretto ai dati dei pazienti, devono assicurarsi che l'odontoiatra, nel fornire l'informativa al paziente, non trascuri di indicare che i dati saranno oggetto di trattamento da parte del laboratorio, acquisendo a tal fine il consenso del paziente.
- Per parte sua, l'odontotecnico dovrà assicurare un trattamento dei dati conforme alle disposizioni del Codice e, segnatamente, adottare le misure di sicurezza del caso, diverse a seconda che il trattamento avvenga con o senza l'ausilio di strumenti elettronici.

Riassunto

Le aziende avranno tempo fino al 31/03/2006
Per adeguarsi alle seguenti misure:

- Consegnare lettere di incarico ai dipendenti per i trattamenti consentiti
- Provvedere al periodico aggiornamento (con cadenza almeno annuale) dell'individuazione dell'ambito del trattamento consentito dei singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.
E, se trattano i dati con strumenti elettronici,
- Disporre di un sistema di autenticazione informatica. Questo nel senso che ad ogni incaricato che effettui il trattamento di dati personali con strumenti elettronici dovrà corrispondere un codice per l'identificazione (username) associato ad una parola chiave riservata (password) conosciuta solamente dal medesimo. La parola dovrà essere composta da almeno 8 caratteri (oppure al massimo consentito dallo strumento elettronico) non dovrà contenere riferimenti facilmente riconducibili all'incaricato, ed è modificata, da quest'ultimo, almeno ogni 6 mesi, **3 se si effettuano trattamenti di dati sensibili o giudiziari.**
- In alternativa, il codice prevede altri sistemi di autenticazione, tipo: token, smart card, caratteristiche biometriche.

- 
- Proteggere i dati con l'installazione di antivirus, aggiornati almeno ogni 6 mesi.
 - Predisporre un sistema di blocco tipo "screen saver" per i momenti di "abbandono" della propria postazione di lavoro.
 - Provvedere almeno annualmente all'aggiornamento dei programmi utilizzati con le "patches" rilasciate dai produttori. **Per i dati sensibili o giudiziari l'aggiornamento deve essere semestrale.**
 - Impartire istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con frequenza almeno settimanale.
 - Dotarsi di strumenti anti intrusione per la propria rete aziendale (es. firewall). **Misura necessaria per chi tratta dati sensibili e giudiziari.**
 - Chi tratta dati sensibili con strumenti elettronici è obbligato a redigere il documento programmatico sulla sicurezza almeno annualmente e a citarlo nella relazione accompagnatoria del bilancio d'esercizio, se dovuta.
 - Altre possibili misure: gruppo di continuità, cifratura delle e-mail.