

CODICE DELLA PRIVACY



Contenuti del corso

- Introduzione al nuovo Testo Unico (Codice) sulla Privacy
- Obblighi cui sono sottoposte le aziende - soprattutto per ciò che riguarda gli strumenti elettronici.
- Sanzioni.
- Tempi e modalità di adeguamento.

ITER PER ARRIVARE AL TESTO UNICO

Legge n. 676/96

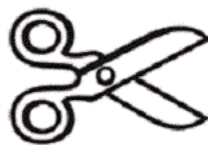
Conferimento dal Parlamento al Governo del compito di emanare un testo unico delle disposizioni in materia di tutela della privacy, in cui fossero inserite tutte le norme vigenti relative al trattamento dei dati personali → *Legge n. 127/2001, art. 1*

Il T.U. doveva essere emanato entro il 31.12.2002

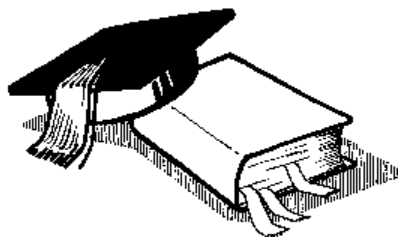
Legge 3.2.2003 n. 14, art. 26

Proroga di 6 mesi il termine (30.6.2003) per l'emanazione del T.U.

Il T.U. è stato approvato dal Governo il 27.6.2003 previa acquisizione dei pareri del Consiglio di Stato e delle competenti commissioni parlamentari → *D.Lgs. 30 giugno 2003, n. 196 (S. O. n. 123/L alla G. U. n. 174 del 29.7.2003)*



**Taglio del 30% delle vecchie norme senza
conseguente maggiore chiarezza!**



Art. 3 (**Principio di necessità** nel trattamento dei dati)

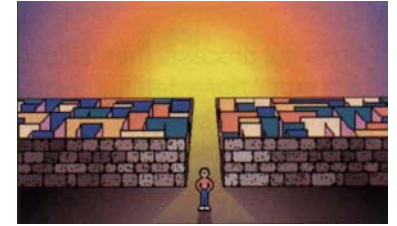
I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità

Il principio della pertinenza e non eccedenza dell'art. 11 del Codice viene anticipato e specificamente rivolto alla configurazione di sistemi informativi e programmi informatici

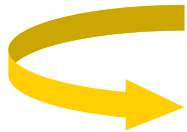


OGGETTO ED AMBITO D'APPLICAZIONE DEL CODICE

La disciplina del Codice (**art. 5**) si estende al trattamento dei dati personali effettuato



- da chiunque (italiano, straniero, europeo) ha sede stabile in Italia (o in luoghi comunque soggetti alla sovranità italiana) anche se i dati sono detenuti all'estero
- da titolari con sede extraeuropea ma che impiegano strumenti – anche non elettronici – situati in Italia (che non siano utilizzati per solo transito)



Il titolare del trattamento designa un proprio **rappresentante** stabilito nel territorio dello Stato

Per i trattamenti effettuati da titolari aventi sede EU la mancanza di norma esplicita trova spiegazione nella direttiva comunitaria a base delle discipline degli stati membri

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:

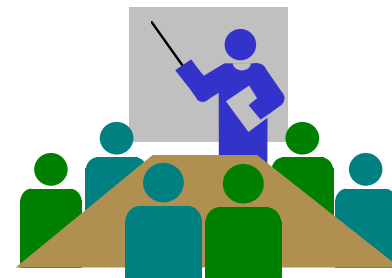
- definitivi di interdizione, inabilitazione e quelli di revoca
- che dichiarano fallito l'imprenditore; di omologazione del concordato fallimentare; di chiusura del fallimento; di riabilitazione del fallito



Comunicazione

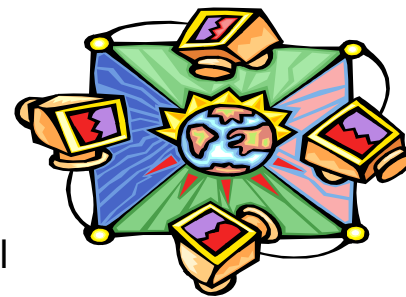
Quando si permette l'accesso ai dati personali ad uno o più "**soggetti determinati**", anche solo ponendo i dati a disposizione o lasciandoli consultare

Non è comunicazione il dare conoscenza dei dati all'interessato, al rappresentante del titolare nel territorio dello Stato, al responsabile e agli incaricati



Diffusione

Quando i dati personali diventano accessibili, in qualsiasi forma, a "**soggetti indeterminati**"; quando cioè ne diventi possibile la conoscenza da parte di chiunque



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

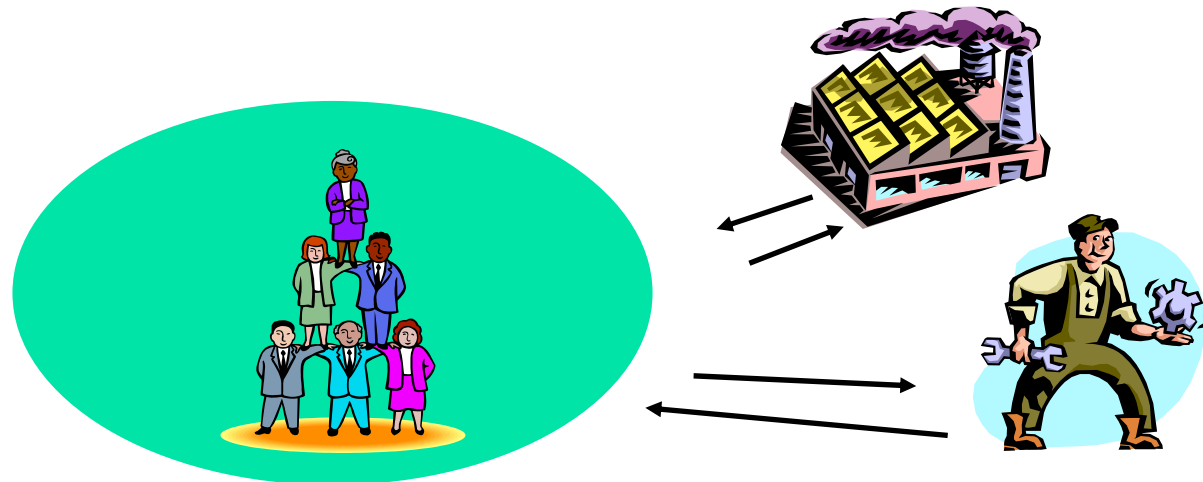
Responsabile del trattamento (art. 29)

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



Interessato e suoi diritti (art. 7)

Persona fisica o giuridica, ente o associazione cui si riferiscono i dati personali

Gli spettano i diritti previsti dall'art. 7 del Codice:

Diritto di sapere se esistono o meno suoi dati presso il titolare

Diritto di ottenere l'indicazione:

- **dell'origine dei dati**
- **delle finalità e modalità del trattamento**
- **della logica applicata nel trattamento effettuato con l'ausilio di strumenti elettronici**
- **degli estremi identificativi:**
 - titolare
 - responsabile se designato
 - responsabile designato dal titolare extra CE stabilito nel territorio italiano
- **dei soggetti o delle categorie ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati**



Diritto di ottenere:

- l'aggiornamento, la rettifica, ovvero l'integrazione dei dati (quando via ha interesse)
- la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati
- l'attestazione che le operazioni dei due punti precedenti sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi (se questo risulta possibile o non sproporzionato)

Diritto di opporsi in tutto o in parte

- per motivi legittimi al trattamento dei dati che lo riguardano ancorché pertinenti allo scopo della raccolta
- al trattamento dei dati personali che lo riguardano ai fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale

I diritti dell'interessato sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile (anche tramite incaricato) alla quale è fornito idoneo riscontro senza ritardo

Cessazione del trattamento (art. 16)

In caso di cessazione (per qualunque motivo) i dati sono:

- distrutti

- ceduti ad altro titolare che li tratti per finalità compatibili con quelle per le quali i dati sono stati raccolti



la “cessione” ad altro titolare per fini diversi è “priva di effetti” (inefficace)

- conservati per fini personali (esclusa quindi comunicazione sistematica o diffusione)

- conservati/ceduti per scopi storici/statistici/scientifici (secondo legge, regolamento, normativa comunitaria, codici deontologici)



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"

Troppo
banale

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

Troppo
dettaglio

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

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

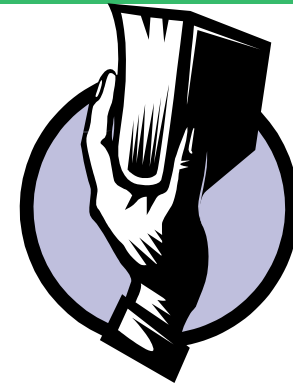
basta un solo nominativo

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**

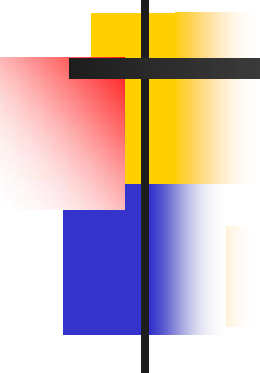




Casi di esclusione consenso in generale e salve le disposizioni per settori specifici (art.24)

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*”

Comunicazione/diffusione dati

Le disposizioni previste dagli artt. 19/21 della L. n. 675/96 sono state comprese solo negli artt. 23.2 e 25

Il loro divieto (nell'art. 25) sembra ridotto in limiti ristretti e cioè per i soli dati:

- per i quali è stata ordinata la cancellazione**
- per i quali sia decorso il tempo necessario al perseguimento dello scopo**
- per finalità diverse da quelle indicate nella notificazione (quando necessaria)**

E' fatta salva la comunicazione/diffusione quando i dati sono richiesti dall'autorità per la difesa/sicurezza dello Stato o per la prevenzione/accertamento/repressione dei reati



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**, allegate 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)

PRESCRIZIONI NORMATIVE

Negli articoli 34-35 il trattamento dei dati è consentito “solo se” sono adottate le misure minime

Art. 35

PER I TRATTAMENTI SENZA AUSILIO DI STRUMENTI ELETTRONICI
Misure minime (nei modi previsti dal disciplinare)

- **aggiornamento periodico dell'ambito di trattamento consentito a incaricati/unità organizzative (p. 27 D.T.)**
- **previsione di procedure per idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti (p. 28 D.T.)**
- **previsione di procedure per la conservazione di atti in archivi ad accesso selezionato; disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati (p. 29 D.T.)**



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



TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Premessa: INCARICATI (art. 30)

- **Designazione scritta del titolare, contenente anche**
 - ✓ **le istruzioni cui debbono attenersi;**
 - ✓ **la precisazione dell'ambito del trattamento consentito (a quali dati possono accedere e quali trattamenti possono effettuare)**

MISURE MINIME PRESCRITTE

➤ **AGGIORNAMENTO ALMENO ANNUALE DELL'AMBITO DI TRATTAMENTO CONSENTITO AGLI INCARICATI**

Si possono fare liste di incaricati per classi omogenee (di incarico e di profilo d'autorizzazione)

➤ **ISTRUZIONI SCRITTE AGLI INCARICATI SU CONTROLLO E CUSTODIA DEGLI ATTI/DOCUMENTI CONTENENTI DATI PERSONALI**

Quando gli atti e i documenti contenenti **dati 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

L'accesso agli archivi **contenenti dati sensibili o giudiziari** è controllato!

Il controllo può avvenire:

- con strumenti elettronici per il controllo degli accessi (utilizzo badge, scanner)
- o da incaricati della vigilanza

- Le persone ammesse, a qualunque titolo, **dopo l'orario di chiusura**, sono identificate e registrate

- Quando gli archivi non sono controllati, le persone che vi accedono sono **preventivamente autorizzate**

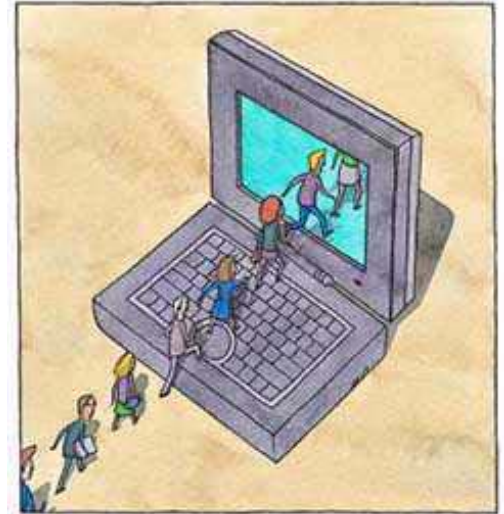


TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Superata la distinzione tra strumenti elettronici collegati a reti e non!

Modalità tecniche da adottare a cura del titolare, del responsabile, (ove designato) e dell'incaricato

Sistema di autenticazione informatica



Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di **credenziali di autenticazione** che consentano il superamento di una **procedura di autenticazione** relativa a uno specifico trattamento o a un insieme di trattamenti

Io sono Tizio!

Io sono Tizio!

Ti riconosco come Tizio

Non ti riconosco


Tizio può accedere alla banca dati

Le credenziali di autenticazione consistono in

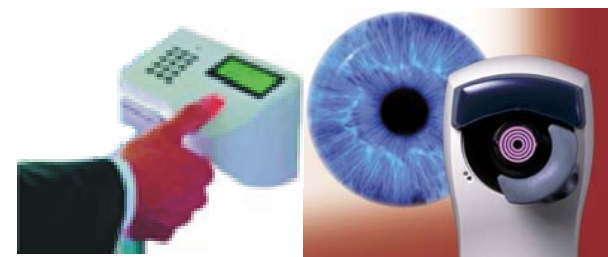
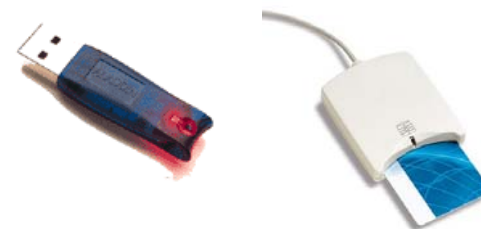
- un **codice** per l'**identificazione** dell'incaricato associato a una **parola chiave riservata** conosciuta solamente dal medesimo (**CONOSCERE**)

- oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave (**POSSEDERE**)

- oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave (**ESSERE**)



Username
Password
Entra



Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato

La **parola chiave**, quando è prevista dal sistema di autenticazione:

- è composta da almeno **8 caratteri**
- oppure, nel caso in cui lo strumento elettronico non lo permetta, da un **numero di caratteri pari al massimo consentito**
- essa non contiene riferimenti agevolmente riconducibili all'incaricato ed **è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi**

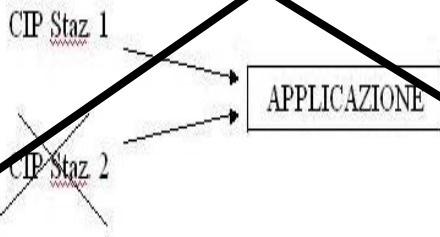
In caso di trattamento di dati sensibili e giudiziari la parola chiave è modificata **almeno ogni 3 mesi**

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate (salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica)

Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali

Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere "contemporaneamente" alla stessa applicazione da diverse stazioni di lavoro (art. 5)



Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento



Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive **disposizioni scritte** volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di **prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema**

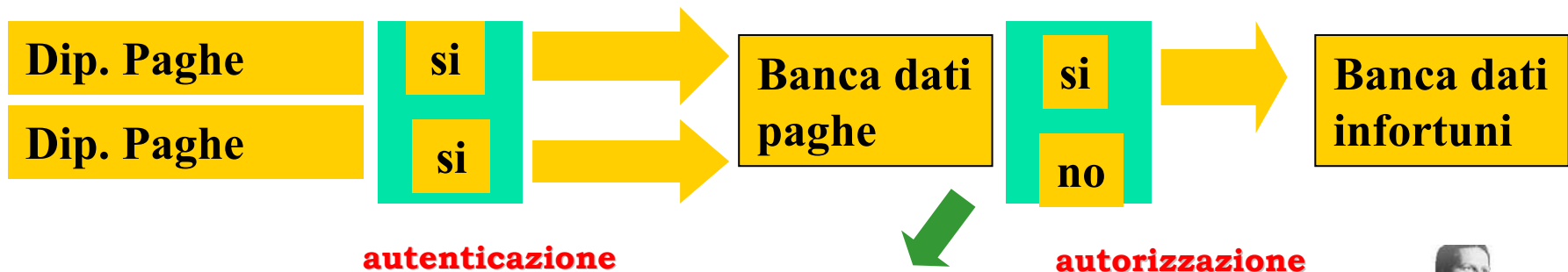
In tal caso la **custodia delle copie delle credenziali** è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i **soggetti incaricati della loro custodia**, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato



Sistema di autorizzazione

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione

I **profili di autorizzazione**, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento



Periodicamente (almeno annualmente) è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione



Con cadenza almeno annuale deve essere individuato l'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici (la lista degli incaricati può essere redatta anche per classi omogenee di incarico)

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici (**antivirus**) da aggiornare con **cadenza almeno semestrale**

Gli aggiornamenti periodici dei **programmi per elaboratore volti a prevenire la vulnerabilità** di strumenti elettronici e a correggerne difetti sono effettuati almeno **annualmente**



trattarsi delle famose patch

Cos'è una patch?

Una patch letteralmente è una "pezza". In realtà è un aggiustamento che le case produttrici di software creano per risolvere bug o problemi al software non riscontrati in fase di testing

In caso di trattamento di **dati sensibili o giudiziari** l'aggiornamento delle patch è almeno **semestrale**

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale



Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici (es.: **FIREWALL**)

Sono impartite 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/giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili

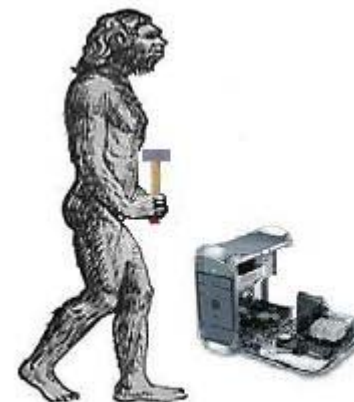


Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni



Misure di tutela e garanzia

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 tecnico (**norma a tutela degli artigiani e delle piccole imprese!**)



SANZIONI PENALI ED AMMINISTRATIVE

SANZIONI AMMINISTRATIVE

• L'organo competente ad irrogare le sanzioni è il **Garante (art. 166)** → COMPETENZA ESCLUSIVA



A

(161) Omessa o inidonea informativa all'interessato: 3.000 → 18.000 €

B

(162.1) Cessione con finalità incompatibile (16.1.b) 5.000 → 30.000 €



SANZIONI PENALI

La condanna comporta sempre la pena accessoria della pubblicazione (art.172)

(167) TRATTAMENTI ILLECITI

Presupposti: dolo e nocumento

Violazione delle norme su:

- (17) Dati quasi sensibili
- (26) Dati sensibili (garanzie)
- (27) Dati giudiziari (garanzie)
- (45) Trasferimenti all'estero
- (25) Comunicazione - diffusione

→ da 1 a 4 anni



- (23) Consenso

• (123-126) Servizi di comunicazione elettronica (obblighi per i dati di traffico e per quelli relativi all'ubicazione)

• (129) costituzione ed utilizzo di elenchi di abbonati

- (130) Comunicazioni indesiderate

→ da 6 mesi a 3 anni

**(168) FALSITA' NELLE NOTIFICAZIONI,
DICHIARAZIONI, ATTI AL GARANTE**

→ da 6 mesi a 3 anni

(169) OMISSIONE DELLE MISURE MINIME



o arresto fino a 2 anni; o ammenda da 10.000 a 50.000 €

E' possibile il “ravvedimento operoso” (169.2).

Viene impartita al colpevole una prescrizione e un termine per la regolarizzazione. Regolarizzazione + il pagamento di 12.500 € → estinguono il reato

(170) INOSSERVANZA DEI PROVVEDIMENTI DEL GARANTE DISPOSTI:

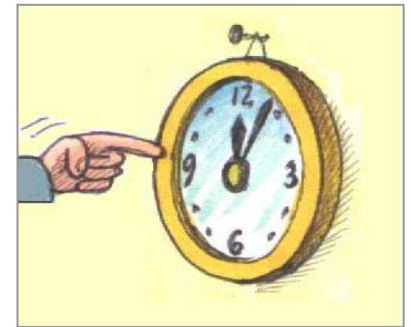
➤ **nelle autorizzazioni al trattamento di dati sensibili/genetici**

➤ **in sede di ricorso (blocco, cessazione)**

➤ **in sede di reclamo (misure opportune, blocco, divieto totale/parziale)**

da 3 mesi a 2 anni

CALENDARIO DI ALCUNI ADEMPIMENTI PER LE IMPRESE



1.1.2004

Entrata in vigore del Codice (informativa/consenso)

31.3.2004

Menzione nella relazione accompagnatoria al bilancio d'esercizio del documento programmatico

entro il 30.4.2004

Notificazioni

30.6.2004

Aggiornamento del documento programmatico da parte di chi tratta dati sensibili/giudiziari con strumenti elettronici

entro il 30.6.2004

Adozione nuove misure minime di sicurezza

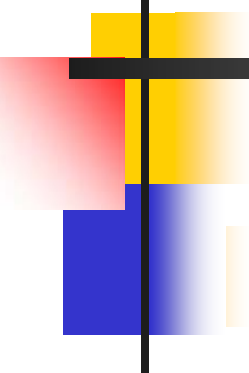
30.6.2004

Scadenza autorizzazioni generali per dati sens./giu.

Riassunto

Le aziende avranno tempo fino al 30/06/2004
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.
- 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 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.
 - Risorse in rete: **<http://www.cedab.com>**



Cedab può aiutarvi ad adeguarvi:

- Predisponendo le credenziali di autenticazione ed i profili di autorizzazione per i dipendenti. (Password – smart card ecc.)
- Installando ed aggiornando gli antivirus e firewall.
- Fornendo gli aggiornamenti (patches)
- Sistemi di salvataggio dati – backup, ripristino, disaster recovery.

Aiutandovi a redigere:

- lettere d'incarico*.
- Informative (anche per mailing commerciale rivolto a potenziali clienti).
- Documento programmatico sulla sicurezza.

Rilasciando un documento che attesti la conformità alle disposizioni di legge.