

# PRIVACY

a cura di **Enrico Pozza**

**CISM**

***e.pozza@flashnet.it***

**www.corporatesecurity.it**

# **INDICE DELLA PRESENTAZIONE**

- 1. Privacy Cosa Significa**
- 2. Il Dlg 196 /2003**
- 3. Metodologia**
- 4. Come Viene Vista la privacy**
- 5. Una Nuova Visione**
- 6. Il Codice in pillole**

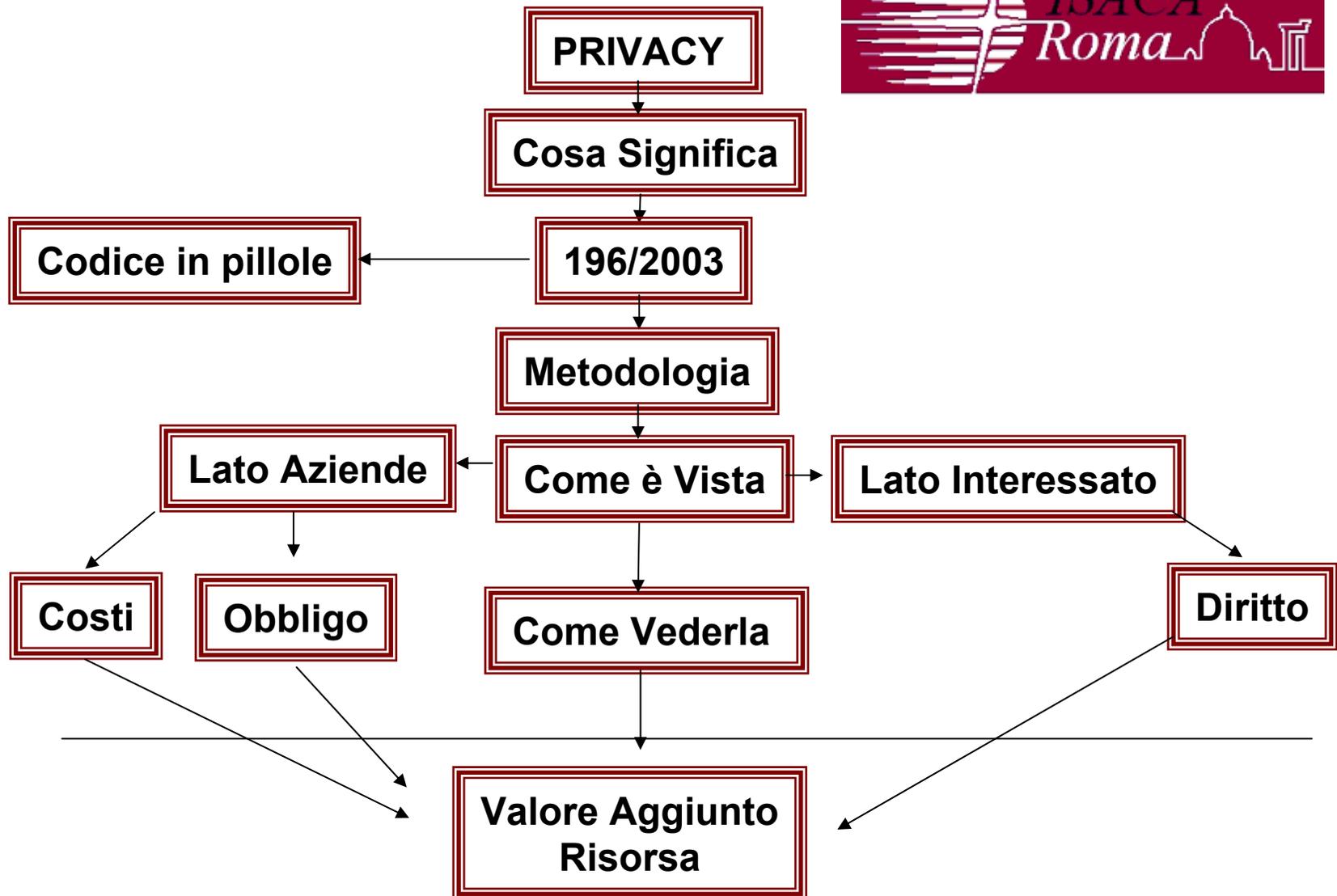
Dal 1 gennaio 2004 è in vigore in Italia

***il Nuovo Testo Unico***

in Materia di Protezione dei Dati Personali

che regola la disciplina sulla privacy,

riaffermando il diritto di ognuno alla protezione delle  
informazioni personali



# Cosa Significa



## PRIVACY

Termine inglese con significati mutevoli, accostabile ai **concetti di "riservatezza", "privatezza"**.

Diritto, alla protezione dei dati personali costituisce **un diritto fondamentale delle persone**, direttamente collegato alla **tutela della dignità umana**, come sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea. (Nizza – Dicembre 2000)

Diritto di controllare l'uso e la circolazione dei propri **dati personali** che costituiscono il **bene primario** dell'attuale società dell'informazione

E' diffusa in tutti gli altri Paesi membri dell'Unione Europea (**direttiva comunitaria 95/46/CE**).



**La PRIVACY coglie “ bisogni sociali ” sempre più diffusi nel mondo occidentale odierno:**

- **Riservatezza**
- **Trasparenza / Fiducia dei rapporti**

**e rappresenta**

- **Una conquista sociale, culturale e politica**

**Da diritto periferico a diritto centrale in vari settori giuridici**



## Normativa Precedente e Europea di Riferimento

- Legge 675 – 31 dicembre 1996** Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
- Legge 676 – 31 dicembre 1996** delega al governo in materia di tutela rispetto ai dati personali
- d.P.R. n° 318 28 luglio 1999**
- Legge 325 - 3 novembre 2000** Disposizioni inerenti l'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'articolo 15 della legge 31 dicembre 1996, n. 675
- Legge n° 127 – 24 marzo 2001** (prevista adozione testo unico)
- 2002/58/Ce 12 luglio 2002** direttiva comunitaria
- Decreto. Legge del 30 giugno 2003 n. 196**

---

## Nuove proroghe

- **31 Dicembre 2005** stesura del DPS
  - **30 Marzo 2006** Adeguamento Misure Minime di Sicurezza
-

# Dlg 196 / 2003

# Da anni di esperienza

Il provvedimento, sulla base dell'esperienza, riunisce in unico contesto i decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni, e contiene anche importanti innovazioni tenendo conto della "giurisprudenza" del Garante e della direttiva europea sulla riservatezza nelle comunicazioni elettroniche.

# Obiettivo

- Il DLG 196/03 ha come obiettivo:

di garantire che il **Trattamento** dei dati personali gestiti si svolga **nel rispetto dei diritti e delle libertà fondamentali dell'interessato**, nonché della dignità sua dignità con particolare riferimento **alla riservatezza**, all'identità personale e **al diritto alla protezione** dei dati personali.

# Destinatari

## A chi si rivolge il decreto?

- Aziende, Imprese, Ditte
- Professionisti, Studi Professionali
- Banche, Assicurazioni
- Organizzazioni ed Esercenti le professioni Sanitarie
- Enti pubblici e Privati
- .....



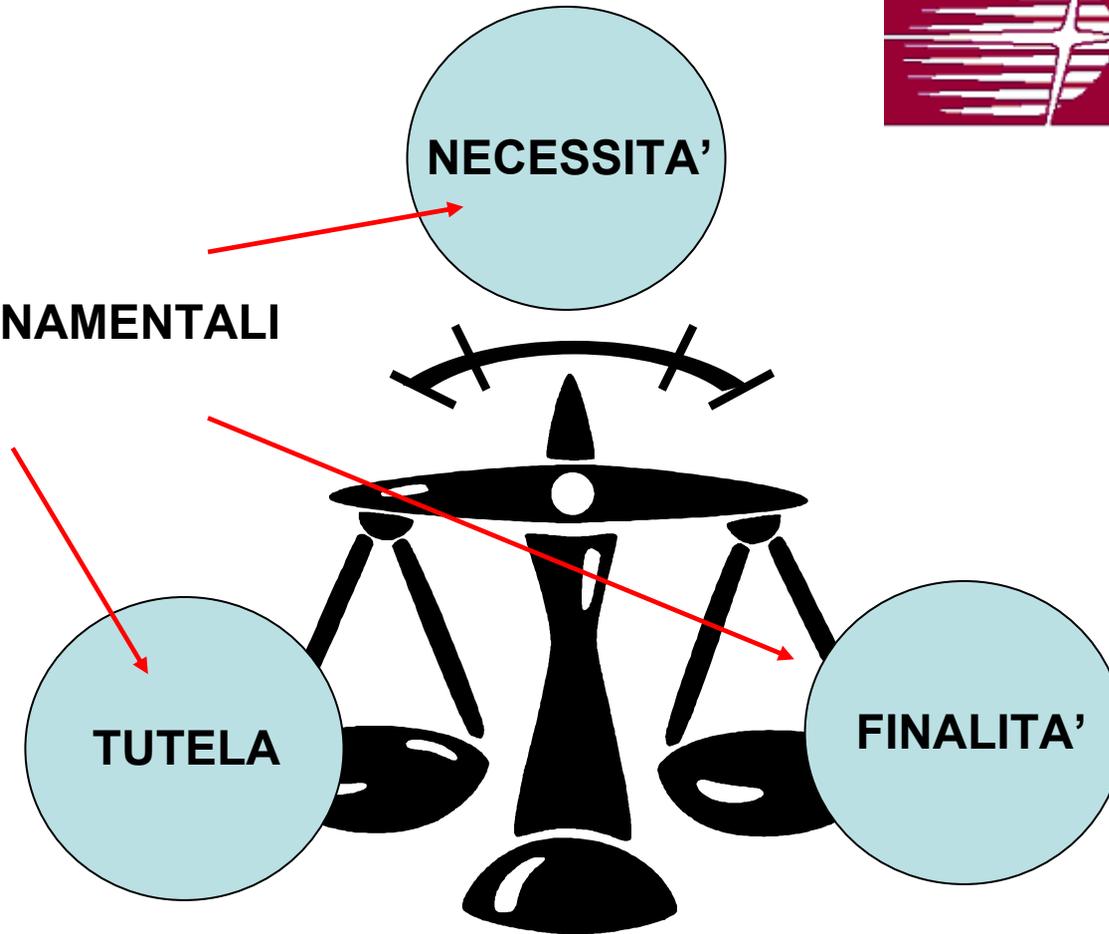
**a Tutti**

# Lo “Spirito”

- Il vero spirito della legge è:

Diffondere la **CULTURA della RISERVATEZZA** e un abitudine a trattare dati personali con cura e sicurezza nel rispetto dell'interessato che deve essere sempre tempestivamente informato sui dati che lo riguardano.

**PRINCIPI FONDAMENTALI**



**PRIVACY**

# Metodologia

- Il Dlg 196/2003 segue i principi fondamentali della Sicurezza dell'informazione ed in particolare i concetti di :
  - Integrità (accuratezza dell'informazione)
  - Confidenzialità (accesso solo alle persone autorizzate)
  - Disponibilità (accesso disponibile quando necessario)

E si richiama gli standard oggi utilizzati nella sicurezza dell'informazione come il BS7799 – ISO/IEC 17799-1

## La storia dello standard

**1995:** British Standard Institution (BSI) pubblica lo standard BS7799-1 “Code of Practice for Information Security Management” derivato da una raccolta di “best practices” prodotta dal DTI (Department of Trade and Industry)

**1998:** BSI aggiunge una seconda parte allo standard intitolata BS7799 - 2 “Part 2: Specification for Information Security Management Systems”

**1999:** BSI pubblica una nuova versione delle due parti dello standard identificate come BS7799 - 1 e BS7799 - 2

**2000:** la parte 1 dello standard BS7799 diviene lo standard internazionale ISO/IEC 17799-1

**2002:** viene pubblica una nuova versione della parte 2, lo standard in relazione al quale vengono rilasciate le certificazioni

## Che cosa sono gli standard BS7799 ?

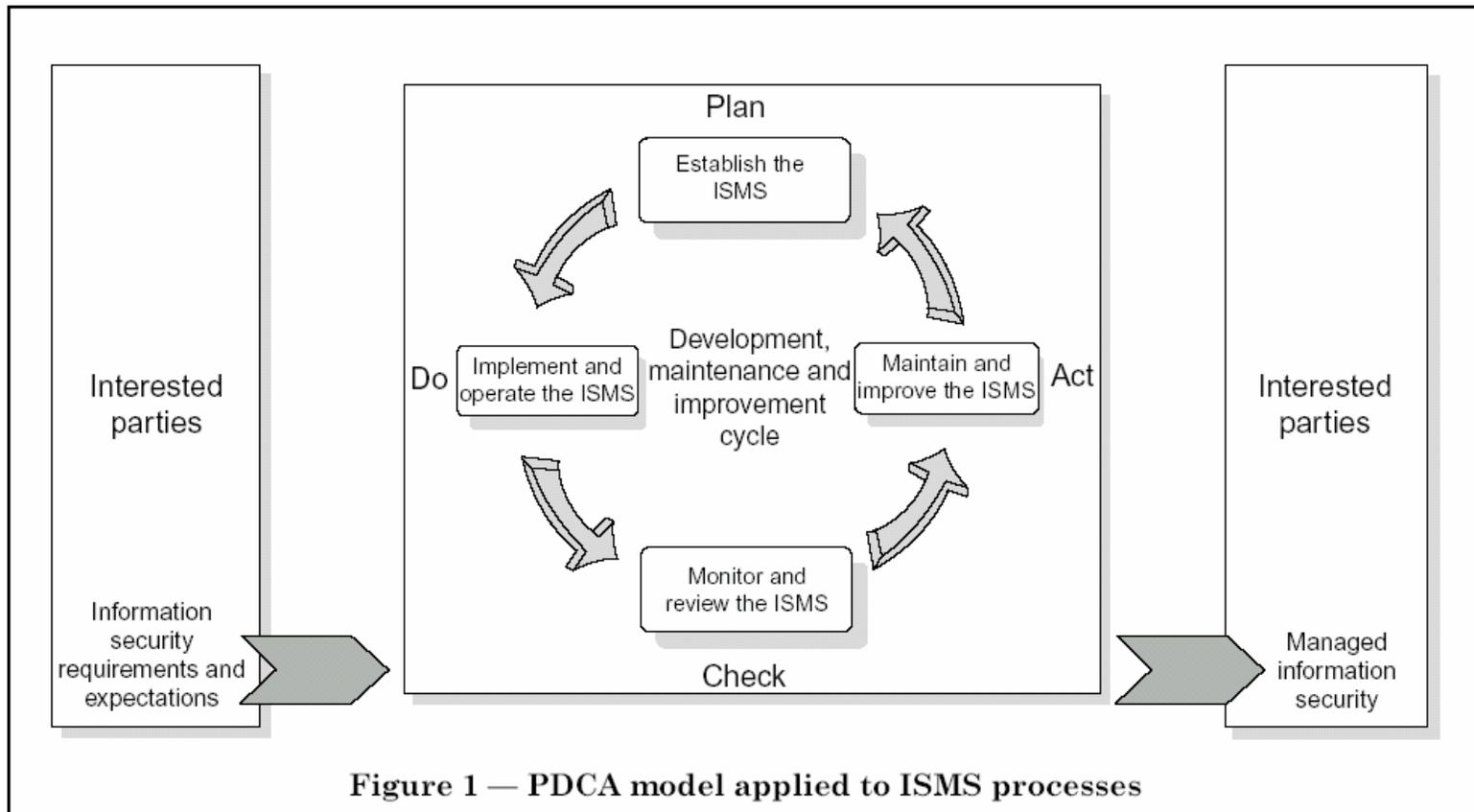
- Un riferimento per capacità di un'organizzazione di tutelare il proprio patrimonio informativo
- *best practice* in materia di sicurezza delle informazioni
- Una metodologia per la gestione della sicurezza delle informazioni aziendali

## Ambito BS7799

La sicurezza non è limitata alla sfera delle tecnologie informatiche

Il sistema di protezione delle informazioni è composto da Componenti logiche fisiche e organizzative

# IL Ciclo PLAN – DO – CHECK – ACT



## PLAN

definizione dell'ambito sistema di sicurezza  
 definizione delle politiche di sicurezza  
 identificazione e valutazione del rischio  
 piano di gestione del rischio

## DO

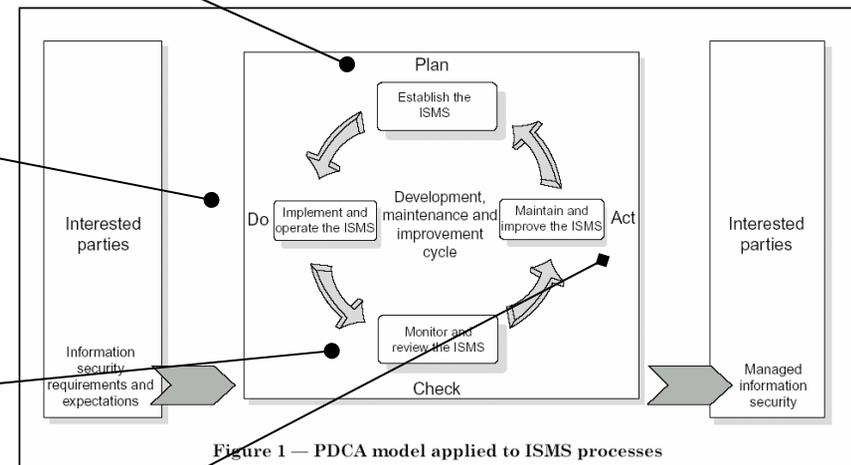
allocazione delle risorse  
 addestramento  
 gestione del rischio

## CHECK

verifica del software  
 verifica delle procedure  
 audit  
 riesame annuale del sistema di sicurezza

## ACT

analisi e azioni correttive e preventive



## IL Ciclo PLAN – DO – CHECK – ACT

### Art. 34 Trattamenti con strumenti elettronici allegato B

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

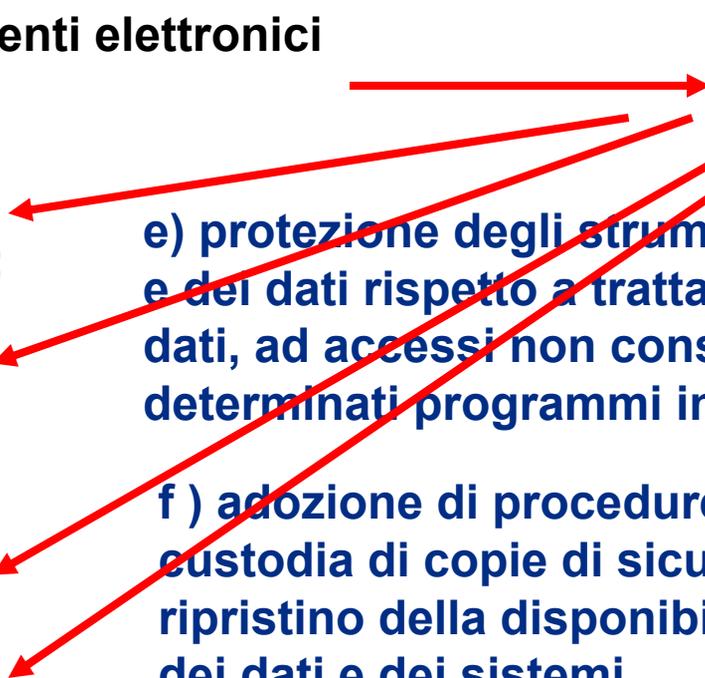
c) utilizzazione di un sistema di autorizzazione;

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.

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

{ Plan  
Do }



**Art. 34 Trattamenti con strumenti elettronici**

**{ Check Act }**

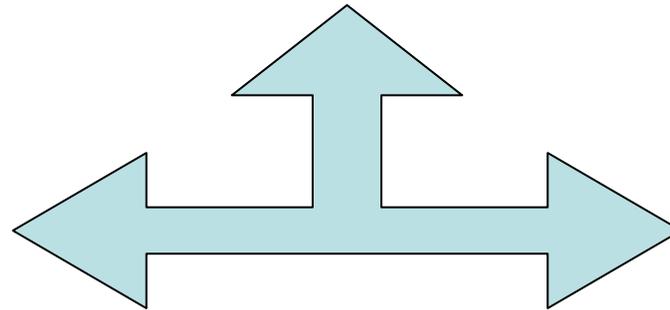
**d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici**

**g) tenuta di un aggiornato documento programmatico sulla sicurezza;**

**Come è  
vista**

**Azienda**

**Interessato**



Allora.....

**Come Vederla**

## Azienda

- **Un obbligo**

**Si crede che la legge costringa le aziende a costosi e fastidiosi adempimenti burocratici**

- **Un costo**

**Il costo della “ Privacy compliance”**

**Il costo della non “ Privacy compliance”**

## Azienda

### I costi

- **Inserimento di risorse umane da destinare alla privacy**
- **Sviluppo e aggiornamento di procedure per la privacy**
- **Formazione**
- **Controllo e audit delle attività inerenti la privacy**
- **Adozioni di strumenti tecnologici ed informatici necessari agli adempimenti**
- **Comunicazione interna per la diffusione delle “PRIVACY POLICY”**
- **Costi di ristrutturazione e riadeguamento dei dati in ottica privacy**
- **Riduzione valore aziendale ( azioni-reputazione-marchio...)**
- **Perdita potenziale di opportunità economiche**
- **Sanzioni amministrative**
- **Risarcimento Danni**

05/01/2004  
Ricette in strada

12/07/2004  
In albergo  
più chiarezza  
nelle informazioni  
ai clienti

14/03/2004  
Dati dei passeggeri aerei  
trasferiti negli Usa: no dell'Europarlamento

18/06/2004  
Il Garante  
corda le condizioni  
per l'invio di Sms  
senza consenso

aziende  
alla r

16/11/2003  
Internet: annunci di lavoro  
a rischi

26/01/2004  
Aziende sanitarie locali e  
21/11/2004

Sanzioni a 11 Asl per trattamenti non trasparenti

16/11/2003  
Anche la pubblicità  
per posta  
deve rispettare  
la privacy

Medici di base,  
consenso e ricette:  
garanzie per i cittadini  
senza burocrazia

occorre maggiore tutela  
per i consumatori

## Interessato

- **Un Diritto**

“...ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano....”

- **Elemento discriminante del mercato**

## Interessato

### I diritti dell'interessato

- ***Diritto di accesso***
- ***Diritto di avere informazioni relative ai dati personali***
- ***Diritto di ottenere la modifica, la cancellazione o il blocco dei propri dati***
- ***Diritto di opposizione***

# Come Vederla

“La società della sorveglianza è resa possibile dalle tecnologie digitali e dalla diffusione di Internet.

**La privacy diventa così una risorsa e uno strumento di competizione economica.**

Per questo motivo, il controllo sui dati personali è al centro di un conflitto che vede come protagonisti le imprese, lo stato e i singoli. “

Un'intervista a Stefano Rodotà

La corretta applicazione consente non solo di adempiere agli **obblighi di legge**, ma anche di **vedere la Privacy** come:

- **una Leva operativa**
- **un Vantaggio Competitivo**
- **un Valore aggiunto**

## una **Leva Operativa**

- per sviluppare ad innalzare la soglia di fiducia dei consumatori nei confronti delle aziende
- per proteggere i dati aziendali il modo efficace
- per mantenere la qualità e affidabilità dei dati aziendali
- per la segretezza delle informazioni aziendali

## un Vantaggio Competitivo

- migliorare l'organizzazione aziendale
- ottimizzare i processi di lavoro
- operare nella consapevolezza che i dati trattati siano corretti, integri, aggiornati – *come richiesto dal Codice all'art.11*
- che i dati costituiscano vere informazioni d'impresa.

---

**“...rende possibile all'impresa una presa di coscienza di quanto possiede e della sua rilevanza ai fini dello svolgimento dell'attività economica..”**

---

## Un Valore Aggiunto

- la conoscenza e consapevolezza
- la protezione del Business
- la qualità

---

**“..La privacy vista come qualità: un marketing aziendale che miri solo ai clienti disponibili a saperne di più su quei determinati prodotti, di fatto rispettandoli e valorizzandoli. E, così facendo, dimostrando in questo modo riguardo per la propria stessa sopravvivenza..”.**

rif. Da Costo a Risorsa a cura di Gaetano Rasi

**“.....La tutela della privacy, a fronte della sua onerosità, consente, quale valore aggiunto, un complesso processo di inventario e di riordino dell’intero patrimonio informativo dell’azienda. Ciò rende possibile all’impresa una presa di coscienza di quanto possiede e della sua rilevanza ai fini dello svolgimento dell’attività economica...”**

**rif. Da Costo a Risorsa a cura di Gaetano Rasi**

**mente,  
ta come  
effettivamente  
consente di guadagnare  
la fiducia del consumatore, può rendere**

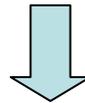
**“....possiamo leggere questo metodo di analisi come uno strumento utile a garantire che i processi di lavoro d’ufficio siano sempre più affidabili, più sicuri e più efficienti. Infatti, il Dpss ha lo scopo di eliminare gli sprechi di tempo, e quindi diminuire i costi, dovuti ad errori, rielaborazione o reinserimento di dati persi e a ripetizione di trattamenti errati .....”**

**WWW.CNA.IT**

**Si avrà quindi la garanzia di :**

- **ottemperare alla legge**
- **operare in sicurezza**
- **godere della piena fiducia della propria clientela.**

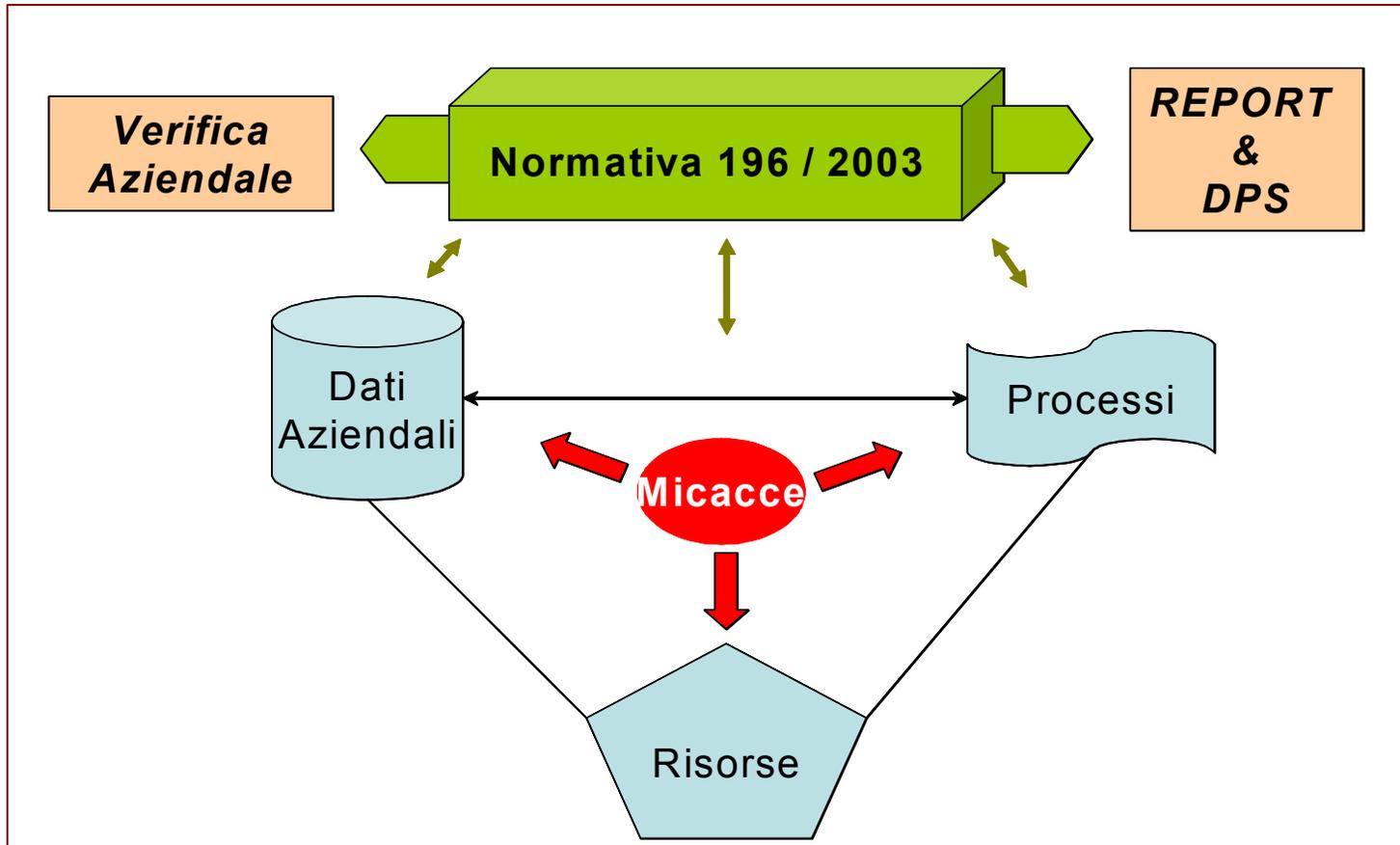
**In tal modo la PRIVACY si trasforma  
da costo a investimento**



**PUNTO DI CONVERGENZA TRA  
SVILUPPO DELLE AZIENDE E CRESCITA CIVILE**

# Come fare Privacy

# Modello di riferimento



## Processo della Privacy



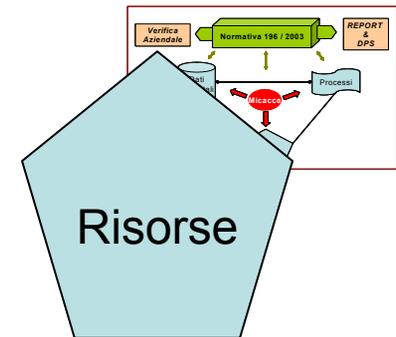
## Identificare la sicurezza dei dati

- sotto gli aspetti di
  - **Sicurezza organizzativa:**
    - attraverso l'individuazione di procedure e standard,
  - **Sicurezza fisica:**
    - Attraverso l'insieme delle misure di protezione dell'archivio che contiene i dati trattati;
  - **Sicurezza logica:**
    - Attraverso l'identificazione della garanzia di integrità, affidabilità e segretezza dei dati;
- **Gli aspetti informatici sono trasversali** rispetto a questa suddivisione: infatti possono toccare aspetti sia organizzativi sia fisici sia logici.

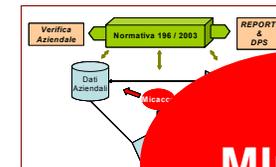
## Definire l'organizzazione

Sono identificate le seguenti figure:

- Titolare
- Responsabile
- Incaricato



## Verifica delle minacce



**Minacce**

Il titolare di qualunque tipo di trattamento dati ha l'obbligo di proteggere i dati che l'interessato gli ha affidato ...

- ...da intrusione
- ...da distruzione
- ...da manipolazione

# Analisi dei Rischi

Identificazione dei rischi per

- **Ridurre al minimo l'utilizzo dei dati personali**
- **Ridurre il rischio di distruzione anche accidentale, dei dati**
- **Ridurre il rischio di perdita anche accidentale, dei dati**
- **Ridurre il rischio di accesso non autorizzato**
- **Ridurre il rischio di utilizzo non consentito**
- **Ridurre il rischio di trafugamento di dati**
- **Ridurre il rischio di utilizzo non conforme alla raccolta**

# Misure di Sicurezza

Responsabilità Civili

Misure di Sicurezza

Responsabilità Penali

Misure idonee

Misure Minime

Danni causati dal trattamento

Obblighi Di Sicurezza Art. 33

Trattamenti con Strumenti elettronici

Allegato Tecnico B  
Punti 1 26

Trattamenti con Strumenti cartacei

Allegato Tecnico B  
Punti 27 28

*Misure Minime di sicurezza*

*la mancata adozione comporta sanzioni per il Titolare e Responsabile*

## Schema delle Misure di Sicurezza

	Archivi <u>Solo</u> Cartacei	Archivi Elettronici
Dati Sensibili	Misure Minime	DPSS
<u>Solo</u> Dati <u>non</u> Sensibili	Misure Minime	Misure Minime

# Tempistica

## *Ogni anno*

- Verifica ambito di trattamento consentito ai singoli incaricati
- Verifica sussistenza delle condizioni per la conservazione delle autorizzazioni per l'accesso ai dati particolari per gli incaricati
- Verifica istruzioni organizzative e tecniche affinché il salvataggio dei dati sia effettuato settimanalmente
- Programmazione interventi di formazione per gli incaricati del trattamento
- Aggiornamento delle "patch" dei programmi per computer, nel caso di trattamento di dati comuni (n. 17, Allegato B)

# Tempistica

## Ogni sei mesi

- Aggiornamento dei software antivirus, per tutti i tipi di dati (n. 16, Allegato B)
- Aggiornamento delle "patch" dei programmi per computer, nel caso di trattamento di dati sensibili (n. 17, Allegato B)
- Cambiamento passwords (se dati comuni)

## Ogni tre mesi

- Cambiamento passwords (se dati sensibili)

# Tempistica

## Dopo sei mesi

- Disattivazione credenziali di autorizzazione se non utilizzate (n. 7, Allegato B)

## Ogni settimana

- Salvataggio dei dati (n. 18, Allegato B)

# Tempistica

## Entro 31 marzo dell'anno in corso

Aggiornamento del Documento programmatico sulla sicurezza

Verifica caratteristiche responsabili

Verifica mantenimento incaricati  
Programmazione formazione

Verifica misure di sicurezza

(nota per 2005: aggiornamento alle nuove misure di sicurezza entro 30 giugno 2005)

# Codice in pillole

- **L'art. 1** del Codice della Privacy recita infatti che “***chiunque ha diritto alla protezione dei dati personali che lo riguardano***”.
- **L'art. 2** del Codice della Privacy, recita “ *il trattamento dei dati personali 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*” e assicurando “*un elevato livello di tutela dei diritti e delle libertà*”
- **L'art 3** | **sistemi informativi e i programmi informatici sono 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.



## Trattamento dati ↔ Attività Pericolosa

Il Testo Unico qualifica il trattamento dei dati come attività pericolosa (art. 15)

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 natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.

## **Adempimenti essenziali minimi**

coinvolgono tutti i destinatari della normativa

- **Notificazione Preventiva**
- **Informativa *ex art. 13***
- ***Consenso***
- ***Nomina degli “incaricati”***
- ***Nomina del/dei responsabile/i***
- ***Adozione delle misure minime di sicurezza***
- ***Redazione del Documento Programmatico sulla Sicurezza (DPS)***

A ciò si aggiungono **ulteriori adempimenti** quali a titolo esemplificativo:

- Verificare i dati personali trattati e controllare la pertinenza e la non eccedenza degli stessi rispetto alle finalità della raccolta;
- Controllare l'esattezza dei dati personali
- Conservare i dati personali per il periodo di tempo necessario agli scopi per cui sono stati raccolti,
- Rispondere tempestivamente alle richieste degli interessati:
- Aggiornare semestralmente i software antivirus
- Aggiornare annualmente (entro il 31 marzo di ogni anno) il DPS;
- Rivedere annualmente il piano di formazione degli incaricati;
- Fornire indicazioni nella relazione al bilancio d'esercizio circa la redazione o aggiornamento del DPS.

## Documento Programmatico di Sicurezza

**Deve contenere:**

**1. Elenco dei trattamenti effettuati**

- **Archivio dei dati**
- **Struttura che effettua il trattamento**
- **Posizione dell'archivio**
- **Contenuto**
- **Informazione particolari legate al trattamento**

**2. Struttura delle responsabilità**

**3. Analisi dei rischi**

**4. Elenco delle misure di sicurezza adottate**

**5. Procedure di salvataggio e ripristino**

**6. Iniziative formative**

# Sanzioni

Il Codice della Privacy prevede in caso di violazione delle relative disposizioni le seguenti sanzioni:

- civili
- amministrative
- penali

# Sanzioni

## Civili

L'art. 15 del Codice della Privacy dispone che **“chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile”**.

L'onere della prova è pertanto a carico del titolare, del responsabile, dell'incaricato chiamato a rispondere dei danni i quali dovranno dimostrare di aver adottato tutte le misure idonee.

E' previsto il **risarcimento sia del danno patrimoniale sia del danno non patrimoniale** anche in caso di violazione dell'art. 11 del Codice della Privacy sulle modalità di trattamento e sui requisiti dei dati.

# Sanzioni

## Amministrative

Sono considerate sanzioni amministrative :

- La omessa o inidonea informativa relativa a trattamenti che ***non contengono dati sensibili***

**Ammenda da 3.000,00 € a 18.000,00 €**

*Tale somma può essere aumentata fino al triplo se, in ragione delle condizioni economiche del contravventore, risulta inefficace.*

# Sanzioni

## Amministrative

Sono considerate sanzioni amministrative :

- La omessa o inidonea informativa relativa a trattamenti che ***contengono dati sensibili***

**Ammenda da 5.000,00 € a 30.000,00 €**

*Tale somma può essere aumentata fino al triplo se, in ragione delle condizioni economiche del contravventore, risulta inefficace*

# Sanzioni

## Amministrative

Sono considerate sanzioni amministrative :

- La omessa o incompleta notificazione  
**Ammenda da 10.000,00 € a 60.000,00 €**

# Sanzioni

## Penali

Sono considerate sanzioni penali:

Il trattamento dei dati senza il prescritto consenso

- se il trattamento causa un danno
  - **reclusione da 6 a 18 mesi;**
- se il trattamento è effettuato in violazione delle regole in ordine alla comunicazione ed alla diffusione:
  - **reclusione da 6 a 24 mesi**

# Sanzioni

## Penali

Sono considerate sanzioni penali

La violazione dei divieti di comunicazione e diffusione:

- se il trattamento causa un danno:
  - **reclusione da 1 a 3 anni**

# Sanzioni

## Penali

Sono considerate sanzioni penali

- La omessa adozione delle misure minime di sicurezza:
  - **arresto sino a 2 anni**
  - **ammenda da 10.000,00€ a 50.000,00€**

# Organi di Controllo

- Ufficio del garante
- Guardia di finanza

# Riferimenti



- *Da Costo a Risorsa a cura di Gaetano Rasi Garante della Privacy 2004*
- *Inside 1to1 Privacy Larry Ponemon 2002*
- *Privacy, Consumers, and Costs How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete Robert Gellman 2002*
- *Organization for Economic Cooperation and Development, Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 20 I.L.M. 422 (1981), O.E.C.D. Doc. C (80) 58 (Final) (Oct. 1, 1980),. An Assessment of the Costs of Proposed Online Privacy Legislation (2001)*
- *Ernst & Young, Customer Benefits of Information Integration by Financial Services Companies 5 (2000)*
- *Commission of the European Communities, Unsolicited Commercial Communications and Data Protection at 66-67 (2001)*
- *GAO Identity Fraud*
- *The Pew Internet & American Life Project, Trust and Privacy Online: Why Americans Want to Rewrite the Rules at 10 (2000)*
- *The Paradoxical Value of Privacy Paul Syverson Naval Research Laboratory March 14, 2003*
- *The Value of privacy Engineering Steve Kenny and John Borking PISA Consortium\*Dutch Data Protection Agency 2003*
- *The Role of Information in Lending: The Cost of Privacy Restrictions Loretta Nott, Government and Finance Division 2003*
- *The Paradoxical Value of Privacy Paul Syverson Naval Research Laboratory 2003*

## WWW

[www.garanteprivacy.it](http://www.garanteprivacy.it)

[www.cna.it](http://www.cna.it)

[www.confindustria.it](http://www.confindustria.it)

[www.actonline.org](http://www.actonline.org)

[www.pewinternet.org](http://www.pewinternet.org)

[www.coe.int](http://www.coe.int)

[www.europa.eu.int/eur-lex](http://www.europa.eu.int/eur-lex)

[www.europa.eu.int/index\\_it.htm](http://www.europa.eu.int/index_it.htm)

[www.europa.eu.int/comm/](http://www.europa.eu.int/comm/)

[ue.eu.int/it/summ.htm](http://ue.eu.int/it/summ.htm)

[www.europarl.eu.int/home/](http://www.europarl.eu.int/home/)

[www.privacy.it](http://www.privacy.it)

[www.privacy.org](http://www.privacy.org)