Nuovo Codice della Privacy

Decreto L.vo 196/03

SalvoReina

LE MISURE MINIME DI SICUREZZA

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza

Excursus della legge ed evoluzione delle "Misure Minime"

La prima legge sulla Privacy la Legge 675/96
Istituito nell'anno 1996 l'Istituzione del Garante per la Privacy responsabi
osservanza

La 675/96 stabiliva concetti fondamentali in merito al diritto di chiunque alla riservatezza alla riservatezza e alla tutela dei dati personali

La 675/96 stabiliva le "misure minime" di sicurezza necessarie per effettuare i trattamenti (DPR 318/99)

C'era una volta la tutela del dato…

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

Misure Minime di Sicurezza

Excursus della legge ed evoluzione delle "Misure Minime"

Durante gli anni, ci sono stati centinaia di pronunciamenti tesi a chiarire o meglio specificare gli ambiti di applicazione

Nel 2004 la vecchia 675/96 è stata sostituita dal "testo unico" approvato a giugno 2003 che riorganizza la materia accogliendo in se tutti i pronunciamenti del Garante

La nuova legge dà inoltre attuazione alle direttive 1996/45/CE e 2002/58/CE del Parlamento Europeo e del Consiglio

Evoluzione indotta da pressioni geo-politiche : il dato personale come un bene della comunità

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

Misure Minime di Sicurezza

Excursus della legge ed evoluzione delle "Misure Minime"

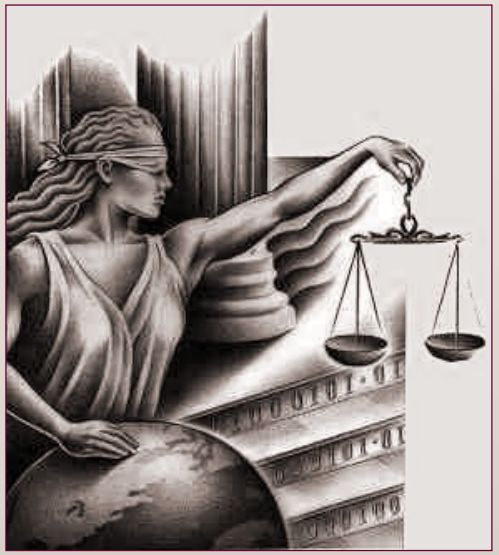
Legge 675/96 - cosiddetta Legge della Privacy

- La tutela delle persone e soggetti terzi rispetto al trattamento dei dati personali
- In vigore dall'8 Maggio 1997
- Comunicazione al Garante entro 30 Dic 2000
- Obbligo delle "Misure Minime di sicurezza" stabilite con il DPR 318/99
- Abrogata da 31 Dic 2003 in favore del Nuovo Testo Unico

Evoluzione indotta da pressioni geo-politiche : il dato personale come un bene della comunità

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



Misure Minime di Sicurezza

Excursus della legge ed evoluzione delle "Misure Minime"

Legge 675/96 - cosiddetta Legge della Privacy

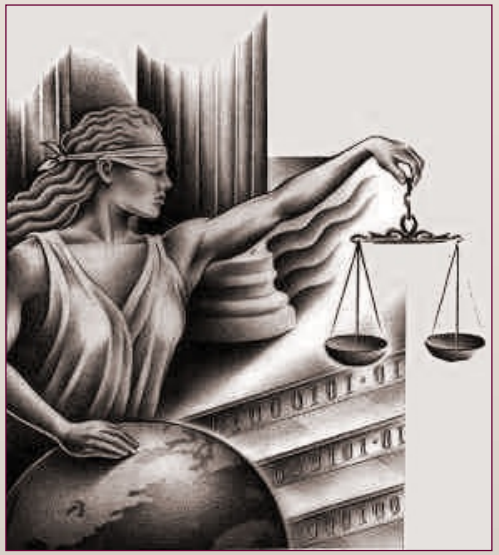
- Applicata anche alle reti interne
- Prevedeva sanzioni penali
- Faceva riferimento per la responsabilità al **Art. 2050 CC**
- Richiedeva livello di controllo e di protezione "allo stato dell'arte"

Anche se attenutata dalle circolari esplicative, un ordinamento molto rigido!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



Misure Minime di Sicurezza

IL NUOVO TESTO UNICO

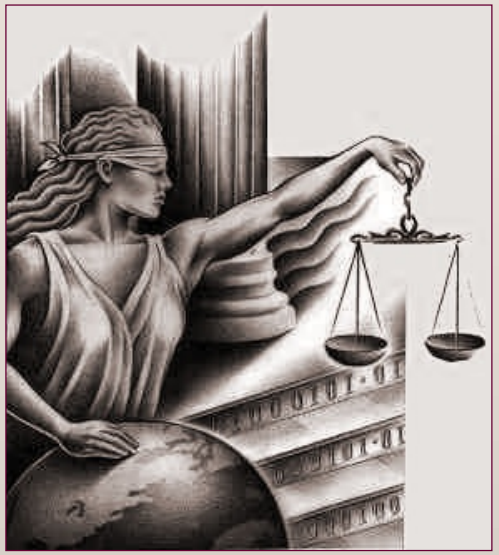
Decreto legislativo 30 Giugno 2003, n. 196
"*Codice in materia di protezione dei dati personali*"

- Pubblicato G.U. n. 174 del 29 Lug 2003
- In vigore dal 1 Gen 2004
- Consta di 186 articoli e 3 allegati
- Ha abrogato la legge 675/96 aggiornandola e incorporandovi organicamente i pronunciamenti emessi nel tempo dal Garante
- Sanzioni fino a 90 Keuro di multa e 3 anni di carcere
- Vige il richiamo all'art. 2050 CC

Ancora una legge molto dura

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



Misure Minime di Sicurezza

COSA E' CAMBIATO?

Legge 675/96

Regolamento delle misure minime

- Emesso tre anni dopo la legge (DPR 318/99)
- Introduceva norme ridicole e incomprensibili

Tre scenari nebulosi previsti

- Trattamento dati presonali non in rete
- Trattamento dati presonali effettuato in rete
- Trattamento dati sensibili effettuato in rete

Definizione di trattamento "in rete" largamente discussa e polemicamente affrontata da giuristi mentre pretestuosamente semplificata dai System Manager sul campo

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

Misure Minime di Sicurezza

COSA E' CAMBIATO?

DPR 318/99 - Lettera A

- **Trattamento dei dati non in rete**

- **Parola chiave per accesso ai dati**
- **Individuazione per iscritto dei soggetti preposti alla loro custodia**
- **Individuazione per iscritto dei soggetti che hanno accesso ad informazioni che concernono la medesima**

Scarse indicazioni e istruzioni confuse sulla redazione dei documenti cartacei : un festival di pre-compilati

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

Misure Minime di Sicurezza

COSA E' CAMBIATO?

DPR 318/99 - Lettera B

Trattamento dei dati in rete

- **Quanto previsto alla lettera A**
- **Codice identificativo per utente o incaricato**
- **Protezione contro i virus**

Indicazioni tecnologiche vaghe e ambigue sulla dotazione informatica

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza

COSA E' CAMBIATO?

DPR 318/99 - Lettera C

Trattamento dei dati personali "sensibili" con elaboratori in rete

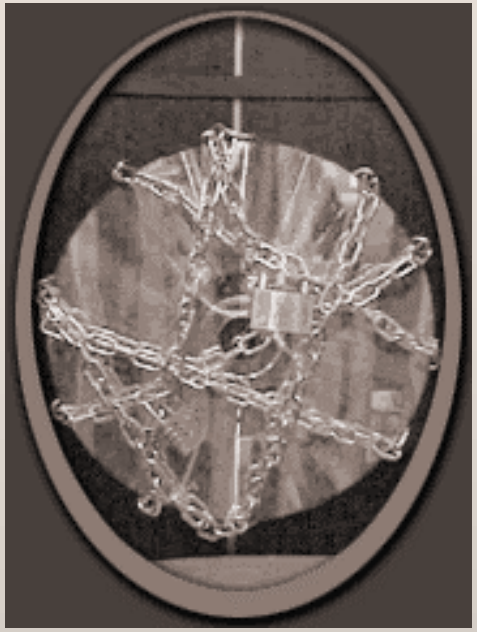
- **Quanto previsto alla lettera B**
- **Accesso autorizzato singolarmente o per gruppo di lavoro**
- **Documento programmatico della sicurezza**

DPS quindi solo associato al trattamento dei dati sensibili!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



Misure Idonee di Sicurezza

ARRIVVIAMO FINALMENTE AL 196/03

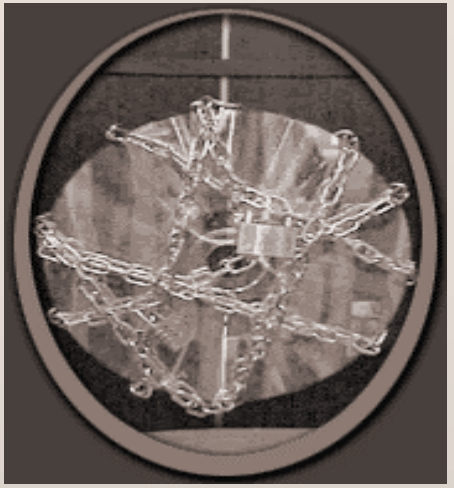
Art. 31 (Obblighi di sicurezza)

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al **progresso tecnico**, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante **l'adozione di idonee e preventive misure di sicurezza**, i rischi di **distruzione o perdita**, anche accidentale, dei dati stessi, di **accesso non autorizzato** o di trattamento non consentito o non conforme alle **finalità della raccolta**.

Dichiarazioni di principio sulla natura dei dati e sulla tipologia in ragione della sostenibilità e del progresso tecnologico

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



Misure Minime di Sicurezza

ARRIVVIAMO FINALMENTE AL 196/03

CAPO II
MISURE MINIME DI SICUREZZA
Art. 33 (Misure minime)

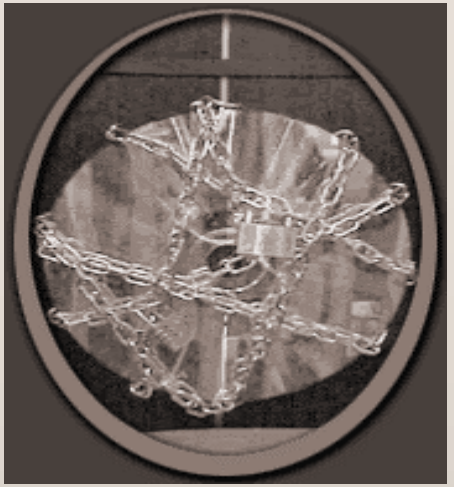
1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

- Trattamenti con strumenti elettronici (Art. 34)
- Trattamenti senza ausilio di strumenti elettronici (Art. 35)

Protezione verso l'esterno ma anche all'inteno!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



Misure Minime di Sicurezza

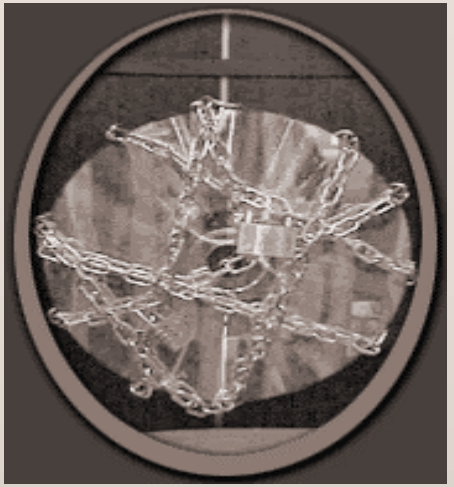
Art. 33 (Misure minime)

- a) autenticazione informatica;
  b) adozione di procedure di gestione delle credenziali di autenticazione;
  c) utilizzazione di un sistema di autorizzazione;
  d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
  e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

Indicazioni puntuali sulle tecnologie e sul loro utilizzo: autenticazione e autorizzazioni con criteri realistici di gestione degli incaricati

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



Misure Minime di Sicurezza

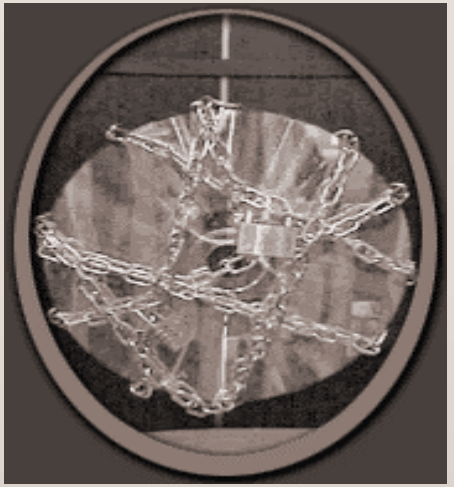
Art. 33 (Misure minime)

- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
  g) tenuta di un aggiornato documento programmatico sulla sicurezza;
  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.

Cifratura: un importante concetto in genere non compreso dai sistemisti (copie di sicurezza, e trasferimento dati)

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



Misure Minime di Sicurezza

ALLEGATO B - DISCIPLINARE TECNICO

RICHIAMATO DAGLI ARTT. 33 FINO AL 36 DEL CODICE

Art. 34 e 35 (trattamenti con e senza l'ausilio di strumenti elettronici)

- Il trattamento di dati personali […] è consentito solo se sono adottate, nei modi previsti dal Disciplinare Tecnico conternuto nell'Allegato B, le misure minime […]

Art. 36 Adeguamento

- Il disciplinare tecnico […] è aggiornato periodicamente in realzione all'evoluzione tecnica

Cifratura: un importante concetto in genere non compreso dai sistemisti (copie di sicurezza, e trasferimento dati)

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza

UNO SGUARDO MIRATO ALL'ALLEGATO B

AUTENTICAZIONE:

si intende una procedura automatica che consenta di identificare l'utente che richiede di accedere al Sistema Informativo

Solitamente si associa un **identificativo pubblico** e una password segreta, ma sono ammesse credenziali biometriche, *token* o una combinazione di essi

Le credenziali devono essere individuali (per incaricato) e gli identificativi devono essere associati biunivocamente e mai riasssegnati in fase di rinnovo

Le password devono essere di almeno 8 caratteri, **non devono essere banali** e devono essere sostituite almeno ogni sei mesi (tre mesi per dati giudiziari/sensibili)

Autenticazione non è un termine di legge (etimol. anglosassone)
Cosa vuol dire password non banali? Biunivocamente?

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

Misure Minime di Sicurezza

UNO SGUARDO MIRATO ALL'ALLEGATO B

Un account va disabilitato quando l'utente non ha più diritto di accesso (licenziamento) o quando è inattivo oltre 6 mesi (aspettative)

Vanno predisposte copie di sicurezza delle password per consentire l'accesso ai dati in casi di **emergenza (key splitting)**

Va predisposta opportuna **formazione** al personale per la sensibilizzazione e l'istruzione ad operare conformemente

Credenziali utente: qualcosa che sa, qualcosa che è, qualcosa che ha!

Sensibilizzazione e istruzione degli incaricati (coerente con fogli di nomina)

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza

UNO SGUARDO MIRATO ALL'ALLEGATO B

AUTORIZZAZIONE:

Per "Autorizzazione informatica" si intende una procedura automatica che consenta di stabilire il diritto di un utente di accedere ad un dato o a un servizio, accordandogli o negandogli l'accesso

Serve un sistema di autorizzazione qualora il tipo di trattamento preveda diversi "profili" di accesso

Occorre procedere almeno con frequenza annuale alla revisione delle liste degli "autorizzati" (*non necessariamente tutti gli incaricati*)

Il sistema di autorizzazione permettere accesso selettivo ai soli dati necessari, ma le modalità di realizzazione non sono imposte dalla leggge (livello applicativo e/o sistema) a seconda delle geometrie architetturali delle banche dati

Spieghiamo la PROFILAZIONE!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza

UNO SGUARDO MIRATO ALL'ALLEGATO B

AUTORIZZAZIONE:

Si deve proteggere i dati contro virus, worm e contro eventuali accessi illeciti (intrusioni) installando o cinfigurando opportuni sistemi di difesa

Antivirus vanno aggiornati almeno ogni 6 mesi

E' obbligatorio provvedere all'aggiornamento dei software utilizzati (patch o service pack) almeno annualmente (semestre per sensibili/giudiziari)

E' necessario effettuare backup dei dati almeno ogni settimana (cifratura quando non prevista dal software di utility!!!)

Non sono scontate le differenze tra ADLS e dial-up

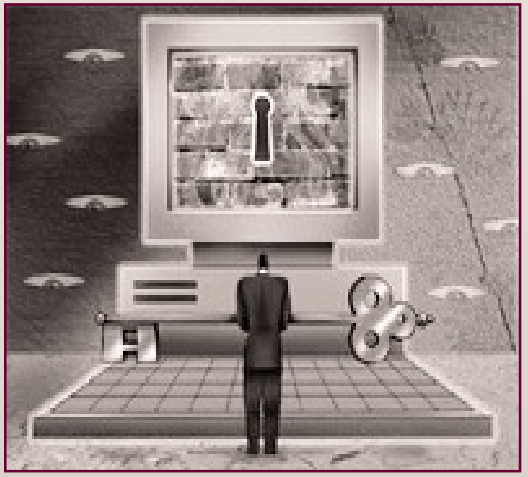
Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza

UNO SGUARDO MIRATO ALL'ALLEGATO B



DOCUMENTO PROGRAMMATICO DI SICUREZZA

Va redatto entro 31 Marzo di ogni anno

Deve dare conto di:

- Trattamenti effettuati
- Distribuzione dei compiti e delle responsabilità
- Analisi dei rischi per i dati soggetti a sensibilità
- Accurata descrizione dei criteri di *disaster recover*
- Piano di formazione del personale secondo competenza
- Applicazione delle misure minime di sicurezza in caso di trattamenti svolti all'esterno della struttura
- Misure di crittografia e cifratura per dati sanitari

DPS è necessario perché esso stesso è Misura Minima di Sicurezza

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

Misure Minime di Sicurezza

UNO SGUARDO MIRATO ALL'ALLEGATO B

MISURE PER DATI SENSIBILI E GIUDIZIARI

- Norme per la custodia dei supporti rimovibili (uso, conservazione e obliterazione)
- Procedure di *disaster recovery* che prevedano il ripristino dell'accesso ai dati al massimo in 7 giorni
- Cifratura dei dati sanitari e loro custodia in locali e/o contenitori di sicurezza

DPS è necessario perché esso stesso è Misura Minima di Sicurezza

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza

UNO SGUARDO MIRATO ALL'ALLEGATO B

MISURE DI TUTELA E GARANZIA

- Nel caso in cui le misure di sicurezza siano implementate o gestite all'esterno. Il fornitore deve rilasciare un attestato di conformita di alla legge

- Chi è tenuto a presentare bilancio ei esercizio deve riferire nella relazione di accompagnatoria dell'avvenuto redazione o aggiornamento del DPS

Di chi fidarsi per la consulenza informatica?
Titolare e bilancio : a regime relativo all'anno precedente?

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

Misure Minime di Sicurezza

SCADENZE NORMATIVE, MODALITA' ATTUATIVE E SANZIONI

Mancata adozione

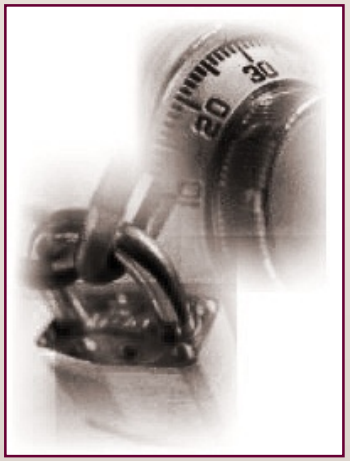
- **Art. 169 (Misure di sicurezza)**
- 1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

Di per se la non adozione è un non adempimento di conformità!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



Misure Minime di Sicurezza

UNO SGUARDO MIRATO ALL'ALLEGATO B

SCADENZE

Tutte le misure indicate nel DPR 318/99 si considerano già in esercizio!

Ogni misura supplementare deve essere posta in atto entro il 30 giugno 2004 (Art. 180.1)

L'impossibilità tecnica di adeguarsi antro il 30 Giugno va dichiarata entro tale data, ed autorizza la proroga al 31 Dicembre 2004

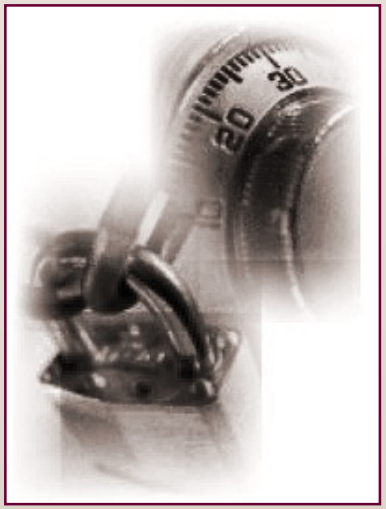
Il DPS va aggiornato netro il 31 Marzo di ogni anno, e le società di capitale devono renderne conto nella relazione annuale di bilancio

Solo per il 2004 il DPS può essere redatto entro il 30 Giugno

A meno di ulteriori provvedimenti sempre possibili…

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



SalvoReina

Cosa fare necessariamente

INNOVAZIONI DEL NUOVO TESTO

Più preciso e circostanziato

- Chiarisce meglio le "finalità" astratte e di principio delle norma a tutela della privacy
- Fornisce indicazionii precise e puntuali per la corretta attuazione delle norme in ogni situazione particolare

Più aggiornato

- Sanziona lo spam!

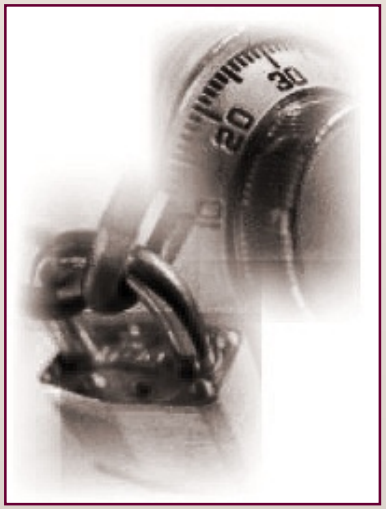
Più tecnicamente valido

- Forte accento sulle questioni organizzative
- Adeguato : "autenticazione" e "autorizzazione" per la gestione degli utenti
- Attento al business continuity e l'asset di azienda (TQM backup/recovery)

Uno strumento aziendale da sfruttare come occasione e non un peso

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



SalvoReina

Cosa fare necessariamente

ANTI VIRUS

- Sempre e comunque, almeno su tutti i client

Firewall

- Se si ha una connessione permanente (adsl) è opportuno inserire un firewall fisico a valle del router
- Su un client può essere sufficiente un *Personal firewall*

Sistemi Windows 95/98

- Vanno bene come client se i dati sono sul server
- Vanno bene anche in rete p2p o con i dati locali a patto che il software applicativo gestisca livelli di protezione

Norme e procedure di sicurezza

- Estese ma ragionevoli, non vessatorie, realmente applicabili

Uno occasione aziendale da sfruttare!!!

Nuovo Codice della Privacy

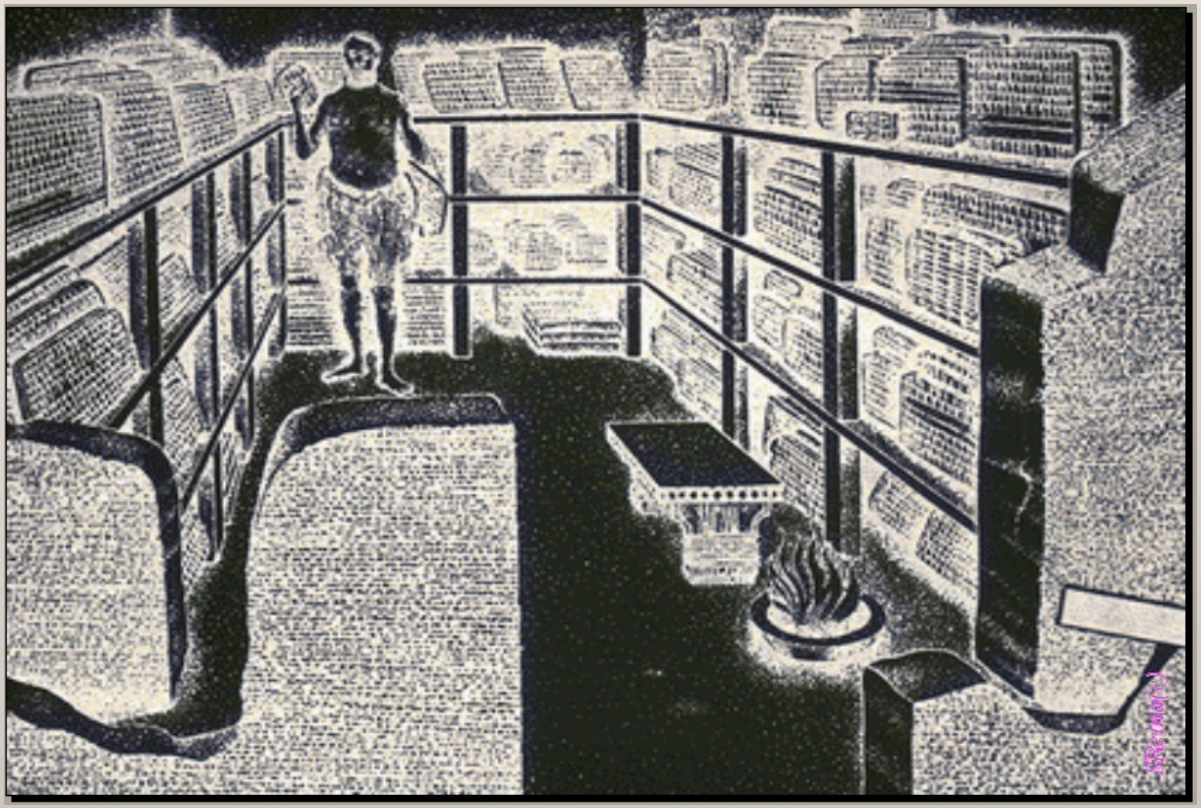
Decreto L.vo 196/03

SalvoReina

DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

Nuovo Codice della Privacy

Decreto L.vo 196/03



Procedure nell'antichità··· perché non og

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

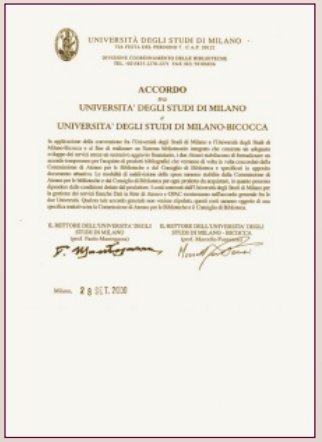
DPS - interrogativi? Perché?

Che cosa è
Come deve essere predisposto
Quali elementi deve contenere
Quale è la valenza ai fini della azienda

Uno strumento aziendale da sfruttare come occasione e non un peso secondo legge e buon senso!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03


UNIVERSITÀ DEGLI STUDI DI MILANO

ACCORDO
tra
UNIVERSITA' DEGLI STUDI DI MILANO
e
UNIVERSITA' DEGLI STUDI DI MILANO-BICOCCA

IL RETTORE DELL'UNIVERSITA' DEGLI STUDI DI MILANO
Prof. Paolo Mantegazza

IL RETTORE DELL'UNIVERSITA' DEGLI STUDI DI MILANO - BICOCCA
Prof. Marcello Fontanesi

Milano, 2 8 SET. 2006

CHI DEVE REDIGERE IL DPS

Art. 34 (Trattamenti con strumenti elettronici)

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), […]

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

Disciplinare Tecnico (All- B), Art 19 (DPS)

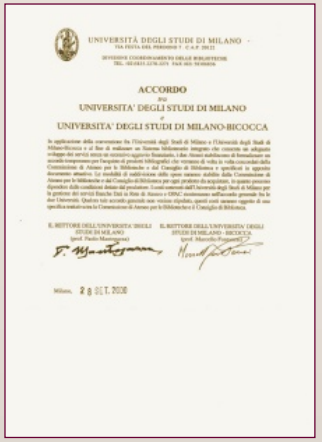
19. […] il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

Chiara implicazione di ruoli: in sede di contraddittorio Art.34<>Art.19

SalvoReina

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



UNIVERSITÀ DEGLI STUDI DI MILANO

ACCORDO

tra

UNIVERSITA' DEGLI STUDI DI MILANO

e

UNIVERSITA' DEGLI STUDI DI MILANO-BICOCCA

COSA DEVE CONTENERE IL DPS

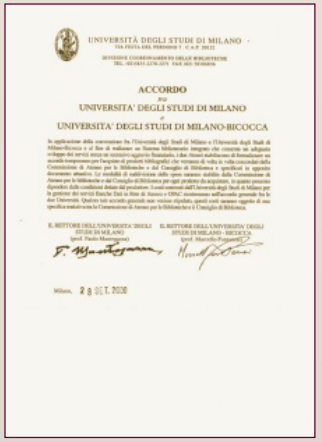
Disciplinare Tecnico (All- B), Art 19 (DPS)

19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità […];
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento
19.6. la previsione di interventi formativi degli incaricati del trattamento […] formazione è programmata
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza […] all'esterno della struttura del titolare;
19.8. […] l'individuazione dei criteri da adottare per la cifratura o per la separazione di dati [sanitari] dagli altri dati personali dell'interessato.

IDONEE: Sufficientemente, sostenibilmente, necessariamente, semplicemente adeguatamente!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03


UNIVERSITÀ DEGLI STUDI DI MILANO

ACCORDO
tra
UNIVERSITA' DEGLI STUDI DI MILANO
e
UNIVERSITA' DEGLI STUDI DI MILANO-BICOCCA

IL RETTORE DELL'UNIVERSITA' DEGLI STUDI DI MILANO
(prof. Paolo Mantegazza)

IL RETTORE DELL'UNIVERSITA' DEGLI STUDI DI MILANO - BICOCCA
(prof. Marcello Fontanesi)

Milano, 2 8 SET. 2006

COME VA GESTITO IL DPS

Disciplinare Tecnico (All- B), Art 19 (DPS)

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza [...]

Disciplinare Tecnico (All- B), Art 26 (Misure di tutela e garanzia)

Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

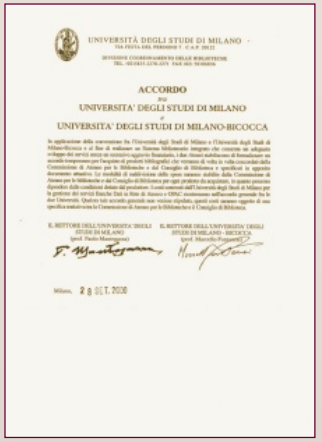
Parere del Garante 22 Marzo

Chiarimenti sulle scadenze e proroga del DPS al 30 Giu 2004

DPS a regime per il bilancio successivo!
Documento vivo non uno scaricabarile!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03


UNIVERSITÀ DEGLI STUDI DI MILANO

ACCORDO

tra

UNIVERSITA' DEGLI STUDI DI MILANO

e

UNIVERSITA' DEGLI STUDI DI MILANO-BICOCCA

IL RETTORE DELL'UNIVERSITA' DEGLI STUDI DI MILANO

IL RETTORE DELL'UNIVERSITA' DEGLI STUDI DI MILANO - BICOCCA

Milano, 2 8 SET. 2006

SalvoReina

INTERPRETIAMO LA NORMA

Il DPS non è un mero adempimento formale piuttosto esso stesso è una misura di sicurezza

Il DPS dovrebbe essere redatto sempre e da chiunque tratti dati personali. anche quando non strettamente previsto dal regolamento

Il DPS è un documento pubblico e comunque ufficiale: la sua mancata redazione, o l'inclusione la suo interno di informazioni non veritiere, configura seri illeciti (*omessa adozione mm, false comunicazioni sociali, …*)

Raccomandabile, pubblico passibile di illecito se ignorato!