Nuovo Codice della Privacy

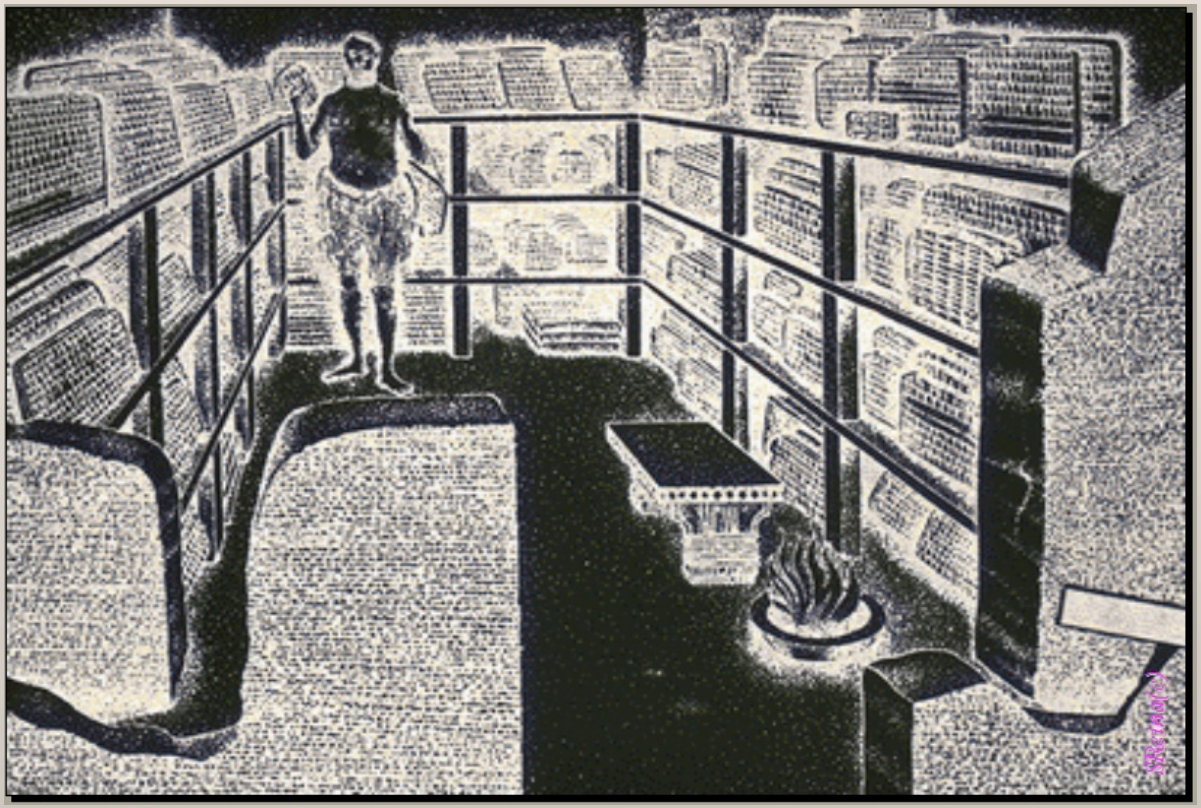
Decreto L.vo 196/03

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

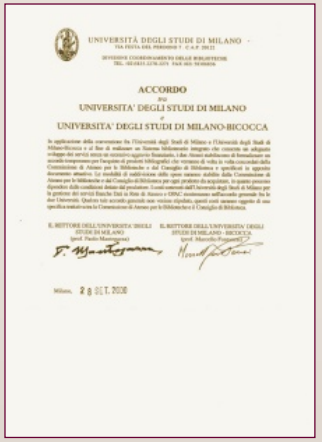
DPS - interrogativi? Perché?

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:

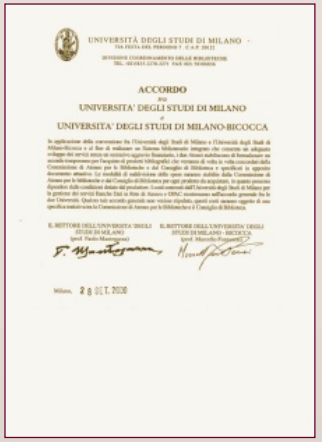
Chiara implicazione di ruoli: in sede di contraddittorio Art.34<>Art.19

SalvoReina

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



UNIVERSITÀ DEGLI STUDI DI MILANO

ACCORDO

tra

UNIVERSITA' DEGLI STUDI DI MILANO

e

UNIVERSITA' DEGLI STUDI DI MILANO-BICOCCA

COSA DEVE CONTENERE IL DPS

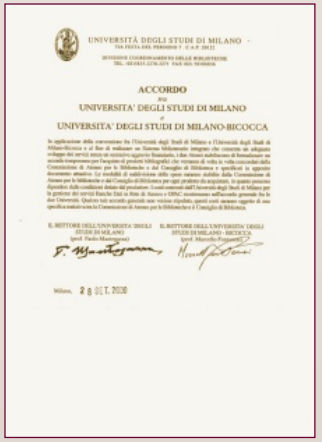
Disciplinare Tecnico (All- B), Art 19 (DPS)

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

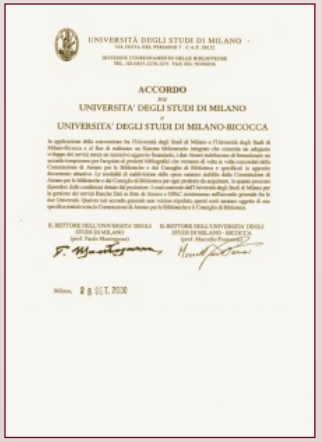
Chiarimenti sulle scadenze e proroga del DPS al 30 Giu 2004

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

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

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

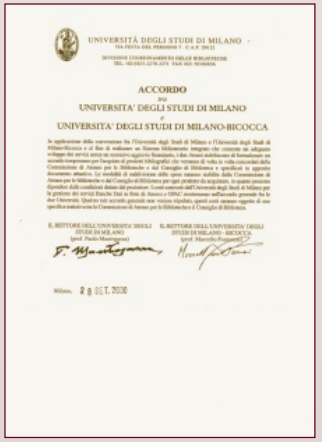
Il DPS dovrebbe essere redatto sempre e da chiunque tratti dati personali. anche quando non strettamente previsto dal regolamento

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!

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

COME CONSIDERARE IL DPS

- UNO STRUMENTO DI LAVORO
- OCCASIONE DI ANALISI DELLE PROBLEMATICHE INTERNE (*QUASI SEMPRE CI SONO E SONO SERIE PER LA PRIVACY*)
- CURATO E CONSERVATO PERCHE' EVIDENZA DELLA PROPRIA SERIETA', BUONA FEDE E SCRUPOLOSITA' (2050 CC)
- NON UN PRECOMPILATO DA RIEMPIRE MA UNA CHECK LIST METODOLOGICO E ORGANIZZATIVA COERENTE CON IL LIVELLO DI PROTEZIONE E PREVENZIONE PER SISTEMI E PROCESSI LEGATI ALLA *POLICY* DELLE *PRIVACY*

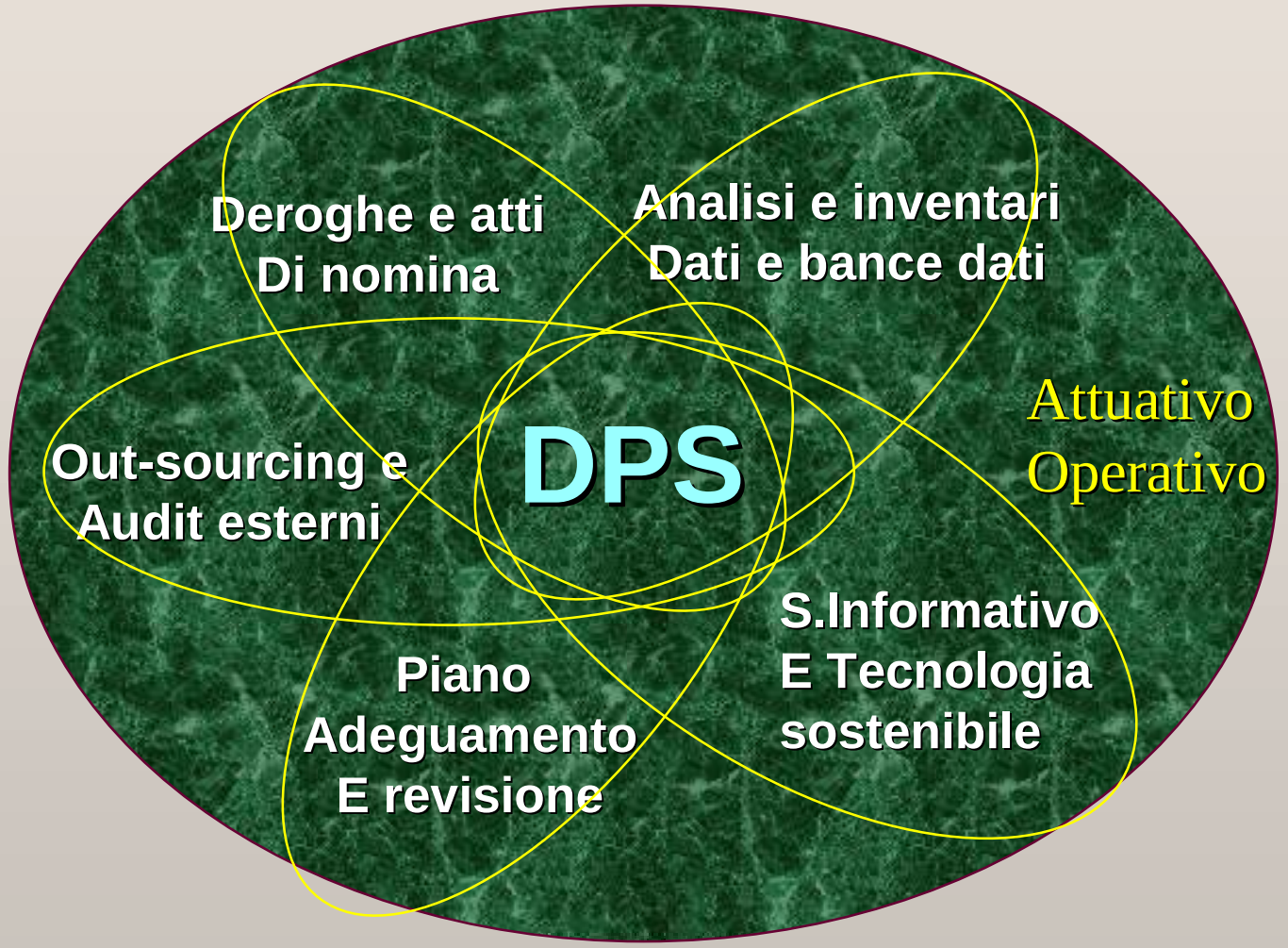
Raccomandabile, pubblico passibile di illecito se ignorato!

SalvoReina

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

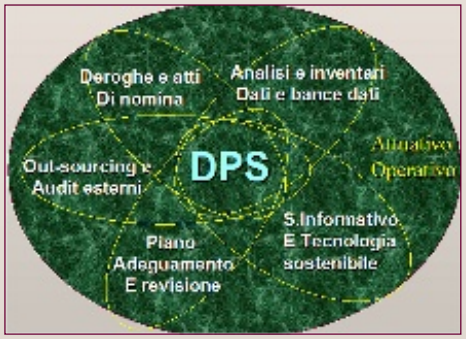


NON ESISTE UN DPS PER TUTTI

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



COME RENDERE CREDIBILE IL DPS

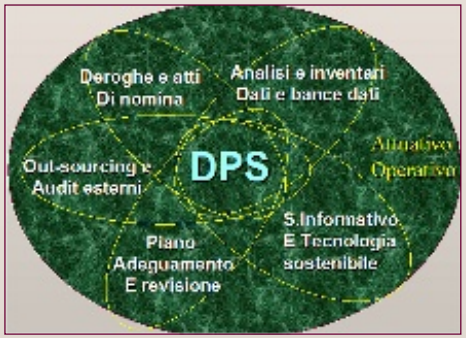
- Non è un semplice adempimento, quindi non può essere un prestampato generico e standardizzato (*a meno di classi di attività corporative*)
- Deve essere fedele e aderente alla realtà della situazione logistica, organizzativa e tecnica sui si riferisce
- L'analisi dei rischi (requisito del nuovo testo unico) rendono non standardizzabile un dps perché le peculiarità da formalizzare sono maggiori delle parti comuni
- Docendo adempiere ad un obbligo meglio farlo bene con una seria riflessione sulla attuazione e la sua opportunità

Analisi dei rischi e profilazione!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



Struttura e contenuti del DPS

- La legge 675/96 e il DPR 318/99 non davano indicazioni sui contenuti lasciando alla sensibilità del titolare

- Risultati precedenti: DPS diversissimi e variegati

- Il DPS del 196/96 lascia massima libertà di decisione, ma indica puntualmente il come operare e quali elementi è necessario trattare

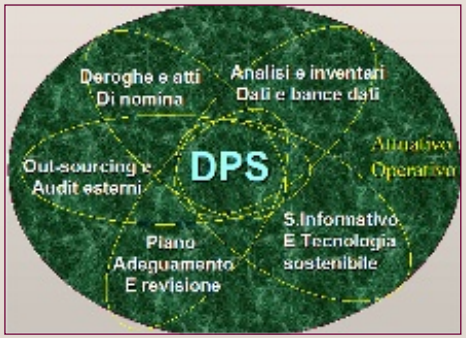
- Una possibile struttura per il nuovo DPS, in attesa di un annunciato modello del Garante, è quindi lo stesso elenco di cui all'Art. 19 in Allegato B

Si è visto tutto e il contrario di tutto!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



ELENCO DEI TRATTAMENTI

Un riferimento incrociato utile anche per la definizione dei ruoli e ledde responsabilità, dei criteri di protezione …

- *Per ciascun trattamento indicare:*
- *Finalità*
- *Modalità di trattamento (durata e tipo)*
- *Categorie di interessati cui il trattamento si riferisce*
- *Indicazione soggetti cui i dati vengono comunicati*
- *Tipo di dati trattati (personali e sensibili)*
- *Responsabile del trattamento*
- *Area organizzativa o ufficio che svolge il trattamento*
- *Nome della banca dati che automatizza il trattamento*

Un elenco dei trattamenti rende credibile l'analisi dei rischi!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

LA STRUTTURA ORGANIZZATIVA

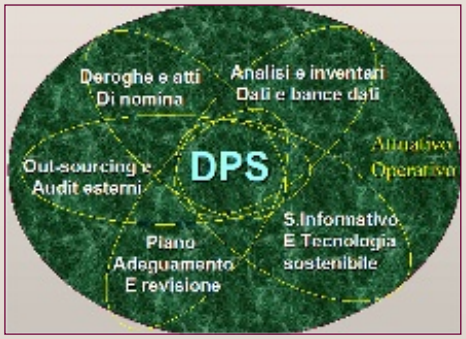
- *Non adottare una gerarchia acritica di figure, ma disegnare una struttura idonea alla reale situazione*
- *Efficace distribuzione dei ruoli senza controproducenti capri espiatori*
- *Coerenza tra il modello e il tessuto organizzativo delle competenze*
- *Ruoli associati in funzioni dove possibile cosi da risparmiare tempo ma rendere più gruppi sensibili*

Non l'organigramma C&P

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



ANALISI DEI RISCHI

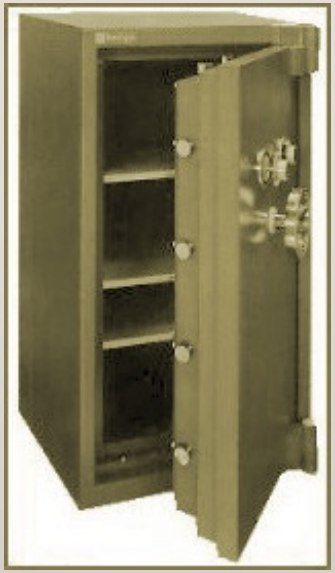
- PROPEDEUTICA ALLA SCELTA DELLE CONTROMISURE DI PROTEZIONE
- NON E' NECESSARIO UN ASSESSMENT FORMALE CON STRUMENTI QUANTITATIVI
- UNA SERIA RIFLESSIONE QUALITATIVA CON GIUSTIFICAZIONI COERENTI DELLE SCELTE
- ELEMENTI DA CONSIDERARE
  - Identificazione *Asset* da proteggere
  - Identificazione di minacce e vulnerabilità
  - Probabilità di accadimento
  - Quantificazione dell'impatto in caso di accadimento

Fondamentale, semplice non formale

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina



Le misure di sicurezza adottabili

Descritte sia quelle già adottate che in predicato se . richieste per migliorare il livello di protezione sulla base dell'analisi di rischio

CLASSI DI MISURE

- FISICHE (antiintrusione, ant-iincendio, comtinuità servizi)
- LOGICHE (password, autenticazione e autorizzazione)
- ORGANIZZATIVE (controllo di accesso ambienti, conservazione documenti)

Indicare il responsabile che controlla l'efficacia e l'effettiva attuazione delle misure

Descrivere ciò che viene fatto e non ciò che "si dovrebbe fare"

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

I CRITERI DI *DISASTER RECOVERY*

Misure tecnico-organizzative aventi come scopo il ripristino in tempi brevi della operabilità in caso di disastri gravi (incendi,)

Tre tipologie di misure

- **Fisiche**: linee di backup, locali ignifughi, gruppi di continuità
- **Logiche**: sistemi di alta disponibilità, ridondanza dei dati (RAID e repliche)
- **Organizzative**: backup remoti, procedure manuali…

Due possibili piani di azione (non esclusivi)

- *BCP (Business continuity Plan)*
- *DRC (Disaster Recovery Plan)*

Ricordare il criterio di sostenibilità per le Piccole e Micro aziende!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

LA FORMAZIONE COME ADEMPIMENTO

La consapevolezza e la collaborazione del personale sono critici per il successo e la funzionalità di ogni piano di sicirezza

Educare e istruire gli utenti è indispensabile (*oltre che necessario!*)

La formazione è imposta sui soli incaricati, ma è chiaro che anche gli altri addetti dovrebbero essere al corrente della politica dulla privacy

Più cicli di formazione *ad hoc* andrebbero pianificati:

- **Formazione specifica per incaricati**
- **Formazione e sensibilizzazione per personale in generale**
- **Formazione e affiancamento per Amministratori di Sistema (consulenza ICT)**
- **Formazione e affiancamento per Titolari e responsabile (consulenza sulla norma)**

Consulenza e formazione non insieme ma abbinabili

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

I TRATTAMENTI ESTERNI (out-sourcing)

Nel caso in cui l'azienda si avvalga, in tutto o in parte, di soggetti terzi per effettuare i trattamenti è necessario armonizzare le regole che regolano il rapporto contrattuale col fornitore

Una chiara distribuzione di compiti e di responsabilità in relazione al trattamento dei dati personali (*dove, come e quando*) per definire la zona di interfaccia tra interno/esterno

Occorre descrivere reciprocamente :

- ***Responsabili coinvolti (nomine e accettazioni iscritto)***
- ***Limiti di responsabilità assunti dal fornitore (attestato)***
- ***Misure di sicurezza del fornitore***
- ***Accordi sul livello di servizio***
- ***Modalità per la verifica dell'operato del fornitore***

Norma orientata al trattamento della comunicazione del dato

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

I DATI SENSIBILI SANITARI

Nel caso in cui l'azienda tratti particolari classi di dati sanitari è richiesta l'adozione di misure di sicurezza molto rigorose

- **Crittografia dei dati sensibili**
- **Conservazione dei dati sensibili in contenitori o locali di sicurezza**
- **Modalità sicure di trasporto (*anche in senso di transazione informatica*)**

In questo caso il DPS deve contenere ulteriori capitoli descrittivi di misure di sicurezza relative a questi presidi.

Norma con implicazioni medico legali comunque applicabili

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

I DATI SENSIBILI SANITARI
Misure di sicurezza

Per dati trattati informaticamente le misure di sicurezza certamente devo comprendere :

- *Protezione da accessi illeciti (intrusione)*
- *Protezione da danneggiamenti intenzionali e non (virus, worm incendi)*

Bisogna quindi descrivere le modalità di adozione di programmi software e sistemi procedurali

- *Antivirus: centralizzati, locali ad accesso controllato*
- *Firewall: di perimetro, di frontiera, con quali regole*
- *Intrusion Detection Systema (solo consigliati)*
- *Intrusione amichevole per monitoraggio sicurezza*

Tutto in armonia con la sostenibilità e la rilevanza del dato protetto

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

L'azienda e il suo dps

Si dovrebbe guardare al DPS non come un costoso e sterile adempimento di legge piuttosto uno strumento di sensibilizzazione per la sicurezza dei processi e la salvaguardia qualitativa del proprio core-business

Il DPS dovrebbe essere redatto per competenze multidisciplinari da un gruppo di *skill* professionali in relazione alla complessità e l'articolazione dei trattamenti

Una volta ultimato deve rimanere vivo e manutenuto secondo necessità di aggiornamento tecnologico e di *business*

Da obbligo di legge a strumento di lavoro!

Nuovo Codice della Privacy

Decreto L.vo 196/03

DPS è una partita a bibliardo a dichiarazione…

Nuovo Codice della Privacy

Decreto L.vo 196/03

SalvoReina

Evitare : gigantismo e nanismo, inutili
Manifestazioni di potenza e fatali vittimismi

SR