CODICE DELLA PRIVACY 2016-17 Data Protection Era

La sicurezza nella gestione di dati e informazioni delle organizzazioni

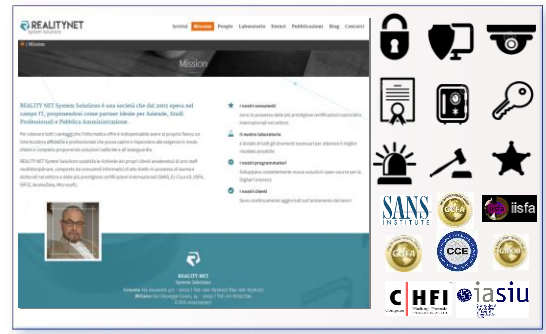
GOVERNO RISCHIO COMPLIANCE
PREPARARE LA MIGRAZIONE
DEL DLG.196/03

Verso il GDPR/16/EU

IL MONDO FUTURO DELLA
Risk Data Management

UNIFICAZIONE
PRIVACY & SICUREZZA ICT

Data Protection : **nuovo paradigma del futuro**

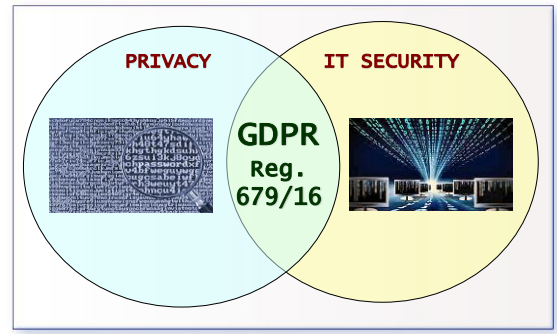


Data Protection : **nuovo paradigma del futuro**

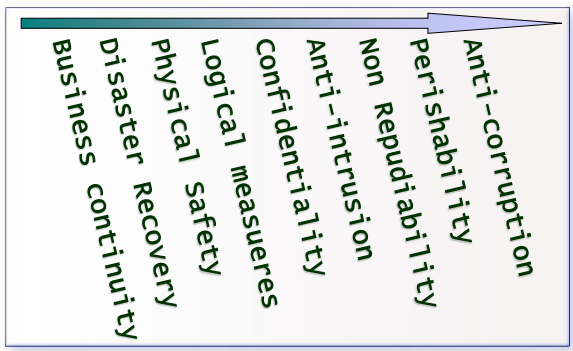
Accortezze per l'esposizione

a) Vibra call / cell silenziato
b) Ridondanza concentrica intenzionale
c) Quali interruzioni possibili
d) Annotazioni per la discussione

Data Protection : **futuro UNIFICATO**
Basta ipocrisie tecnologiche-normative



ICT DATA SECURITY



Data Protection : un **futuro UNIFICATO**
Saggio preliminare su fondamenti e nozioni ICT

TCP-IP MITM	MALWARE ANTIVIRUS
FIREWALL	RANSON'S WARE PLA
MODEM IoT	DB-SERVER
OSI OWASP	NO-SQL DB
BYOD RDP	usb-DRIVE
CLOUD SLA	Sas-sata HD
CYBERSPACE	RJ-45/VPN
WEB 3.0	ROUTER
PLATFORM	WAN-LAN
ERP/CRM	RESILIENZA
Linux/Windows	DHCP-NAS RSA-SHA256

Data Protection : **nuovo paradigma del futuro**

Breve indagine esplorativa, informale e anonima

Quanti consulenti e quante aziende ?

Quanti : ICT, management, legali o proprietà

Quanti tra ICT sono già ADS ?

Quanti tra HR sono già RDT/ODV231?

Quanti della proprietà sono TDT?

Per tutta l'audience : avete mai visto un Sistema Privacy ?

Data Protection : **nuovo paradigma del futuro**

Formazione e aggiornamento

a) Evoluzione della privacy

b) SDP compliance

c) Rischi/sanzioni

d) Paradigmi futuri su CLOUD

e) Verifica Question Time

Data Protection : **nuovo paradigma del futuro**

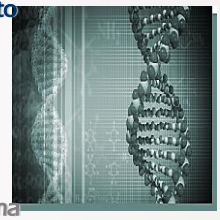
Formazione e aggiornamento

a) Evoluzione della privacy

b) Istruttoria di compliance

c) Rischi e sanzioni

d) Verifica postura del sistema



SalvoReina

Data Protection : **nuovo paradigma del futuro**

Una questione sovranazionale
Un committment forte e distribuito tra le istituzioni

…[come il primo modello di codificazione organica e completa della materia considerata… non solo vale a dare attraverso un nucleo di 185 articoli un rigoroso inquadramento alla disciplina della riservatezza, molteplicità di profili innovativi, direttamente connessi al quadro comunitario e internazionale

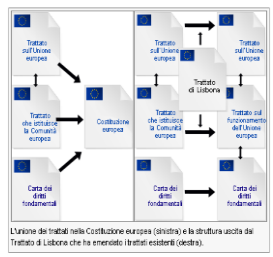
SalvoReina

Data Protection : **nuovo paradigma del futuro**

Regolamento europeo GDPR

il nuovo diritto, così come concepito dalla Carta di Nizza (2000), prima, Trattato di Lisbona (2007) e, ora, dal Codice sui dati personali, sembra il prodotto proprio del "diritto generale della personalità" legato Diritti fondamentali.

Privacy : *non corrisponde necessariamente ad un obbligo di confidenzialità o riservatezza. Nel contesto della direttiva comunitaria, "privacy" indica la disciplina per il trattamento dei dati.*



L'Unione dei trattati nella Costituzione europea (sinistra) e la struttura uscita dal Trattato di Lisbona che ha emendato i trattati esistenti (destra).

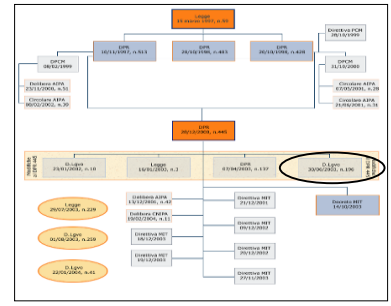
Persona elettronica corrispondente alla nostra identità digitale

Confidenzialità e riservatezza: un diritto non una virtù

SalvoReina

GDPR

Dal 1995 …



Una nuova generazione di norme con giurisprudenza
E sviluppo : Protocollo Informatico e Agenda Digitale

Codice della Privacy

Come siamo arrivati d oggi !


PuntoInformatico

Internet dal 1996

HOME ATTUALITÀ TECNOLOGIA SICUREZZA DIRITTO & INTERNET BUSINESS DIGITAL LIFE

giovedì 10 gennaio 2013

di Mauro Vecchio

Commenti (5)

UE, in pressing per la privacy

Si avvicina la riforma della direttiva sui dati personali che risale al 1995. I parlamentari europei propongono un giro di vite sul trattamento incontrollato da parte delle aziende sul web

Roma - Due proposte di riforma delle regole comunitarie sulla protezione dei dati personali, presentate a Bruxelles dai parlamentari Jan-Philipp Albrecht e Dimitrios Droutsas, a supporto di un contesto "robusto e coerente" per una **maggiore chiarezza legale nelle attività di raccolta e trattamento delle informazioni appartenenti a tutti i cittadini membri dell'Unione Europea**. Ora tocca al commissario alla Giustizia Viviane Reding sottolineare come i membri del Parlamento abbiano mostrato grande compattezza nel seguire gli obiettivi fissati nello scorso anno dalla Commissione Europea: **aggiornare un pacchetto di regole ormai risalente al lontano 1995, prima dell'avvento delle moderne tecnologie digitali**. La definizione di un contesto legale aggiornato risulterà cruciale per il sano sviluppo di un mercato unico nell'era elettronica.

Draft attuativo : 10 Gennaio 2013

Codice della Privacy

Fuoco sulla persona… in che senso

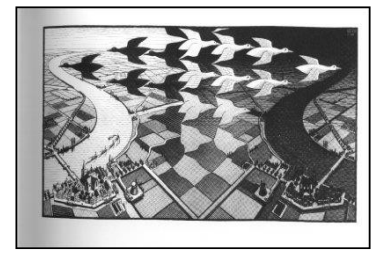
Nuovo Codice della Privacy

Decreto L.vo 196/03

NON fuoco alla persona !

Nuovo Codice della Privacy

Decreto L.vo 196/03



Una difficile migrazione evolutiva

Nuovo Codice della Privacy

Decreto L.vo 196/03

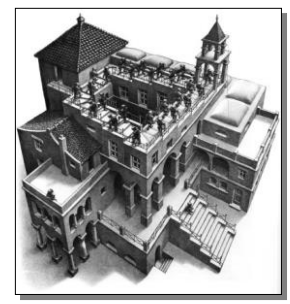
Individuo sociale e non più individuo in quanto singolo,… [il centro di attrazione di una serie di posizioni (variamente definite come diritti civili, diritti sociali, diritti di partecipazioni, ecc.) le quali presuppongono logicamente il rapporto essenziale *individuo-società* e si sviluppano verso il soggetto nella sua specifica qualità di partecipe di determinate comunità, per le funzioni che in esse egli deve esplicare.

Persona elettronica corrispondente alla nostra identità digitale

Adeguamento e non ritardo tecnologico

Nuovo Codice della Privacy

Decreto L.vo 196/03



Paradosso o paradigma : individuo o società ?

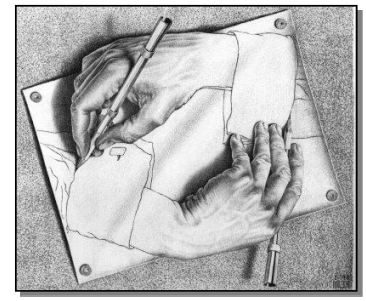
Codice della Privacy

Persona elettronica corrispondente alla nostra identità digitale

Formazione : Cultura aziendale e consapevole

Nuovo Codice della Privacy

Decreto L.vo 196/03 Nuovo Regolamento Europeo



EDUCAZIONE E ATTITUDINE PER AUTOCONTROLLO E AUTOREGOLAMENTAZIONE

Nuovo Codice della Privacy

Decreto L.vo 196/03

Antesignana la Corte costituzionale tedesca che, nel **1984**, dichiarò l'esistenza di "*diritto alla autodeterminazione informativa*", meglio definito come "diritto del singolo a decidere autonomamente quando e con quali limiti possono essere diffuse informazioni riguardanti la propria persona" o altrimenti come "diritto a decidere circa la rinuncia o il trattamento dei propri dati personali".

Concetti di qualità e sicurezza legati alla economia della etica

Costi della non Privacy ! ISO 18000

Nuova Privacy Globale

675/96 → 318/99 → 196/03

Detenzione — Trattamento — Comunicazione/ADS

Evoluzione qualitativa,
tecnologica e culturale risolto dal
NUOVO REGOLAMENTO EUROPEO.

Un problema di competenze multidisciplinari

General
Data
Protection
Regulation

Dec 2015

Data subject
Data controller
Data processor
Personal data

Codice della Privacy

EU Data Protection Laws are Changing

DATA PROTECTION DIRECTIVE 95/46/EC	GENERAL DATA PROTECTION REGULATION (GDPR)
Local laws across 28 member states	One uniform law
Focus on location of equipment	Focus on the data
Multiple Data Protection Authorities	One-stop-shop
Data controllers only	Controllers and processors
Fines differ between countries	Sanctions and large fines
No obligations to report breaches	Obliged to report breaches without delay
No obligation to have a DPO	DPO required for a larger organisation

Una nuova generazione di norme con giurisprudenza E sviluppo : Protocollo Informatico e Agenda Digitale

Codice della Privacy

Fondamenti di Data Protection

dalla Dir 95/46 e GDPR

Accountability : responsabilità globale Titolare politiche sistemiche (**Art. 26**)
Trasparenza : flussi transfrontalieri (periodi di conservazione)
Sistema di gestione : Documentazione (**Art.28**), Struttura org (**Art.3**), deleghe/audit indipendente (**Art.35**)
Sanzioni : fino ad un milione di € e/o 2-3% del fatturato di una *holding* (anche internazionale se sede IT)
Ruoli DP : Joint controllers, nomine di soggetti responsabili interni e/o esterni
Data Protection Officer : **Art. 36**, natura indipendente abche se interno alla organizzazione obbligatorio nella PA e in organizzazioni > 250 dip o > 5000 subject data (**controverso ancora oggi !**)
Audit periodici : Interni e per outsource anche solo indirettamente coinvolti nei trattamenti
Diritto portabilità : migrazioni tecnologiche ICT su Cloud Computing (ITIL, CoBIT e CSA); **Art. 18**
Diritto all'Oblio : Rafforza le facoltà di controllo degli utenti sui propri dati **Art. 17** e **Art. 4 c1** Secure Erasure.
Data Retention : Misure di preservazione del dato degli con adeguamento reale misure di **accesso al dato**

Orientamento dato-centrico : perimetro network IT

Codice della Privacy

SalvoReina

- Si passa dalla previsione di regole formali alla definizione di un sistema di governo sui dati personali basato su tracciabilità
- Sensibilizzazione ed operatività delle funzioni aziendali con maggiore impatto in merito all'utilizzo di dati personali
- Supervisione delle attività cicliche a cura di un responsabile unico
- Creazione di un organo di coordinamento per la gestione del sistema di governo dei dati personali di pertinenza aziendale
- Gestione delle prescrizioni «privacy» secondo l'approccio «PDCA» tipico dei sistemi di certificazione internazionale

Rivoluzione : dalla forma alla sostanza

Codice della Privacy

SalvoReina

Legislazione pensata per qualunque realtà di business

Codice della Privacy

SalvoReina

Non obblighi vessatori ma opportunità e sfida di business

Codice della Privacy

SalvoReina

L'art. 39. Certificazione

- *1. Gli Stati membri, il comitato europeo per la protezione dei dati e la Commissione incoraggiano, in particolare a livello unionale, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento delle operazioni di trattamento effettuate dai responsabili del trattamento e dagli incaricati del trattamento. Si tiene conto delle esigenze specifiche delle micro, piccole e medie imprese. […]*

Chiave del Sistema tracciabilità : TQM e Certificazioni

Codice della Privacy

SalvoReina

L'art. 39 bis. Organismo di Certificazione

- *[…] la certificazione viene rilasciata e rinnovata da un organismo di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati.*
- *Ogni Stato membro stabilisce se tali organismi di certificazione siano accreditati da:*
  - ✔ autorità controllo
  - ✔ organismo nazionale di accreditamento

Chiave del Sistema tracciabilità : TQM e Certificazioni

Nuova Privacy Globale

SalvoReina

General
Data
Protection
Regulation

Dec 2015

Data subject
Data controller
Data processor
Personal data

Glossary :

Security measures, Dissemination, DPAs, DPO, Information Notice, Judicial data, Processing Person Tasked, Sensitive data, Register of processing Operations, One stop shop, Governance & Protection, Security Readiness, Internal Audit & risk management, company culture & awareness …

Data Protection : **nuovo paradigma del futuro**

Ambiti di impatto tzunamico ...

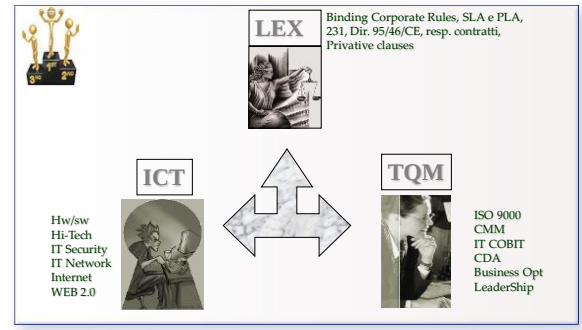
a) Avvocatura – provv. Disciplinari
b) Stampa ed editoria
c) Registro Pubblico delle Opposizioni (abbo
d) Accordi deontologici – Ordini profess.
e) Dati ultra sensibili – indagini giurisprudenz
f) Studi statistici – epidemiologia e censimen
g) Sweet Thirteen: bambini più tutelati
h) Investigazioni – Pari rango
i) Trasmissione dati all'estero (Telco)
j) Gestione privacy negli istituti Religiosi

Casi studio: *Studi legali, Larga distribuzione, Assicurazioni, Banche, Sanità, Sociale*

Nuovo Codice della Privacy

IL DPO FA DA TRAMITE NEL "COACHING" DI INTEGRAZIONE

SalvoReina



Anomalia italia : inflazione di avvocati, giurisprudenza forense

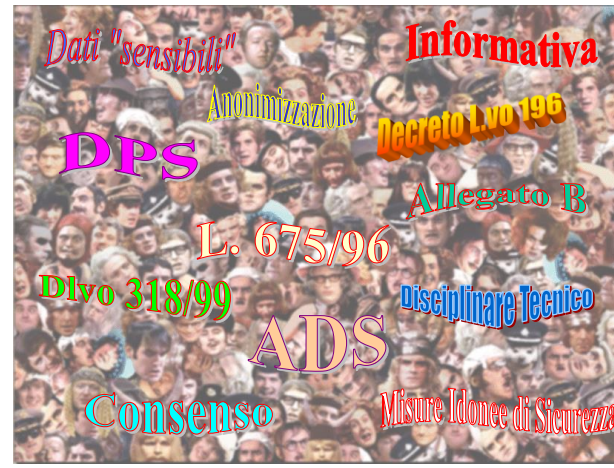
Nuovo Codice della Privacy

Decreto L.vo 196/03

Ora c'è chi controlla !

- ***Oltre 600 provvedimenti***
- ***Oltre 400 controlli***
- ***Oltre 360 ricorsi esaminati***
- ***Circa 4000 reclami, segnalazioni considerati***
- ***43 violazioni di rilevanza giudiziaria***
- ***3 milioni di Euro riscosse al primo trimestre 2010***

Dati ufficiali del garante dal 2009 15% incrementale nell'ultimo report 2014 oltre 5.800K€ comminati.



Nuovo Codice della Privacy

SalvoReina

Quale percorso per approcciare la formazione e la sensibilizzazione ...

Prima di tutto ordine ...
quali nozioni fondamentali sono quelle aggiornate e quali le nuove ?

Nuovo Codice della Privacy

Decreto L.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

Codice quale diritto fondamentale della persona, parallelo col più generale diritto alla riservatezza.

Il legislatore italiano si adegua al quadro della *Carta dei diritti fondamentali del cittadino* europeo ha segnato una dualità di diritti nel Capo II della Libertà

- sia l'art. 7 Rispetto della vita privata e della vita familiare (... Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni);
- sia l'art. 8 *Protezione dei dati di carattere personale*: accesso ai propri dati

Da che parte siamo? Da che parte sono gli altri?

Nuovo Codice della Privacy

Decreto L.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

Oggetto del Trattamento :

qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente mediante riferimento a qualsiasi altra informazione.

*I dati personali si contrappongono ai **dati anonimi**: il dato che in origine o a seguito di un trattamento non può essere associato ad un interessato identificato o identificabile*

Dati Personali, Sensibili, Giudiziari, ultra-sensibili.

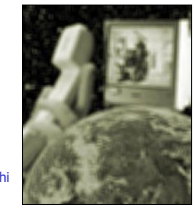
Livellate le differenze della vecchia normativa : ULTRASENSIBILI

Nuovo Codice della Privacy

Decreto L.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

Comunicazione e diffusione del dato!



il Titolo X del Codice italiano, concernente le comunicazioni elettroniche, racchiude una trama normativa di particolare efficacia e completezza, che consente di dare piena attuazione alla direttiva 2002/58/CE.

i dati relativi al traffico; informazioni raccolte nei riguardi **dell'abbonato o dell'utente**; la identificazione della linea; i dati relativi alla ubicazione; le chiamate di emergenza; gli elenchi degli abbonati; le comunicazioni indesiderate; la conservazione dei dati di traffico per altre finalità

garantire i diritti inderogabili delle persone nell'uso dei mezzi di comunicazione elettronica, stabilisce che sono fatte salve le limitazioni derivanti da esigenze ... della riservatezza e protezione dei dati personali **interazione fra due codici, l'uno delle comunicazioni e l'altro della protezione dei dati personali**

Nuovo Codice della Privacy

Decreto L.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

IMPORTANTE NOVITA': DATI INUTILIZZABILI

CAPO I
REGOLE PER TUTTI I TRATTAMENTI

Art. 11 (Modalità del trattamento e requisiti dei dati)

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Dati trattati in violazione alle regole non possono essere utilizzati

Ovvietà : importante che ci sia perché comporta l'autoblocco del dato, quindi una eventuale azione non ha bisogno di ulteriori decreti o provvedimenti specifici. Rif Art. 2050 cc

Nuovo Codice della Privacy

Decreto L.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

Si volta pagina! Forse…

Decreto del nuovo codice è una normativa di seconda generazione (*inibitoria e caducante*)

Raccoglie le esperienze maturate in 16 anni di privacy con una miriade di provvedimenti emanati

Un testo "ridondante" di notevole dimensione, tuttavia chiaro nelle sue linee generali e certamente coerente nelle sue concezioni di adeguamento tecnologico

Nuovo Codice della Privacy

Decreto L.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

PRINCIPI DI NECESSITA' per trattamenti IDENTIFICAZIONE, PERTINENZA e PROPORZIONALITA'

Art. 3 (Principio nel trattamento dei dati)

1. I 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**.

Ad una lettura attenta tutto si risolve individuando chi ha accesso ai dati!

Nuovo Codice della Privacy

SalvoReina

Tipologie di Trattamento :

qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati

La raccolta,	l'estrazione,
la registrazione,	il raffronto,
l'organizzazione,	l'utilizzo,
la conservazione,	l'interconnessione,
l'elaborazione,	il blocco,
la consultazione,	**la comunicazione,**
la modificazione,	**la diffusione**,
la selezione,	la cancellazione.

Critica la cromatura di rischio a seconda delle implicazioni ICT

Nuovo Codice della Privacy

Decreto Lg.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

Diritti dell'interessato

Titolo II
DIRITTI DELL'INTERESSATO
Art. 7 (Diritto di accesso ai dati personali ed altri diritti)
1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

Coerentemente con Art. 1.1 l'interessato è posto come primo interesse rispetto alle disposizioni di trattamento
Rilevante il potenziale onere dei Titolari per le informazioni "**NON**" ancora registrate.

Nuovo Codice della Privacy

Decreto Lg.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

Diritti dell'interessato

Titolo II
DIRITTI DELL'INTERESSATO
Art. 8 (Esercizio dei diritti)

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

Il "**riscontro**" è oggetto di un apposito Articolo 10 che tiene conto delle esperienze maturate.

Va valutato con attenzione perché puo' comportare problemi

Nuovo Codice della Privacy

Decreto Lg.vo 196/03 Nuovo Regolamento Europeo

SalvoReina

Titolo II
DIRITTI DELL'INTERESSATO
Art. 10 (Riscontro all'interessato)
1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare **Idonee e sostenibili** misure volte, in particolare:

a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

Misure "idonee" (termine criticabile, forse adeguate?)
Privato ha interesse all'immagine come valore aggiunto
LE MISURE MINIME SONO RETAGGIO CULTURALE OBSOLETO

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

I DATI SENSIBILI SANITARI
Artt 37 e 38

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.

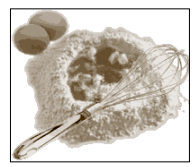
Norma con implicazioni medico legali comunque applicabili

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

NOTIFICAZIONE AL GARANTE
Prima frontiera di credibilità



- ***Categoria e tipo di Dati***
- ***Categoria e tipo di Trattamento***
- ***Categoria e tipo di Interessato***
- ***Categoria e tipo di Modalità***
- ***Categoria e tipo di Finalità***

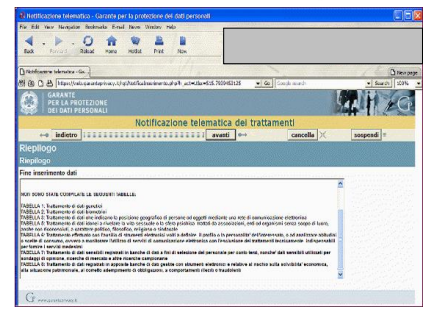
La profilazione standard non esiste !

Delicata alchimia per la interpretazione di merito ai fini della notificazione
Si può ricorrere agli "*intermediari*" per la prassi (*dettagli più avanti*)
Uova, zucchero, farina e acqua in pasticceria!

Nuovo Codice della Privacy

Consulenza del DPO è strategica

SalvoReina



Non esiste più la notificazione preventiva ma esiste la notificazione del DataBreach !

Nuovo Codice della Privacy
Decreto L.vo 196/03

SalvoReina

FIGURE PROFESSIONALI E RUOLI ATTUATIVI E OPERATIVI

Nella futura riforma

Definizioni orientate
Al tipo di Dato trattato

Non si fa sicurezza senza le persone !

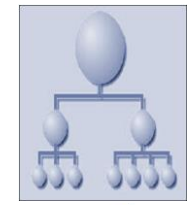
Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

La gerarchia della privacy in azienda

Armonizzare i principi di semplificazione, efficacia e sostenibilità per la identificazione dei ruoli e delle competenze necessarie all'adozione di un sistema virtuoso e credibile di gestione della privacy

- Il Titolare del trattamento
- La nomina de Responsabile
- La nomina / delega dell' ADS
- Designazione degli Incaricati



Nella riforma GDPR-UE
Data Subject
Data Controller
Data Processor

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

IL TITOLARE del TRATTAMENTO
DATA CONTROLLER

Art. 4 lett. F :

"titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni

in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

Persona giuridica e non solo fisica, altro Titolare implicano notevoli possibilità nei casi corporativi e consociate oltre ad un potenziale beneficio di corresponsabilità e logistica delle figure del Responsabile e degli incaricati. (Art.29 e Art. 30)
.

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

IL RESPONSABILE (Anche esterno)
Adesso DPO
Art. 4, lett. g) si intende
"responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo ***preposti dal titolare al trattamento di dati personali****;*

Più preciso all'Art. 29 comma 1 come
Il responsabile è designato dal titolare facoltativamente

Possono essere nominati persone fisiche (interno azienda) o giuridiche (per servizi esternalizzati)

Un Responsabile NON può nominare un altro Responsabile

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

IL RESPONSABILE (Anche esterno)

Come si concretizza il rapporto tra Titolare e Responsabile e cosa vuol dire agire come "*preposto al trattamento*"?

Più preciso all'Art. 29 comma 2.
Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Al responsabile devono essere analiticamente specificati per iscritto "***compiti affidati dal Titolare***" (co.3) e le "***istruzioni***" indicano le responsabilità sulla base delle quali il Responsabile dovrà operare (Art. 29 co.5)

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

L' INCARICATO o Data processor
Art. 4, lett. H) si intende
Sono incaricati
"Le persone fisiche autorizzate a compie operazioni di trattamento del Titolare o dal Responsabile"

Specifica poi l'Art. 30 comma 1 che : l*e operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la* ***diretta autorità del titolare o del responsabile****, attenendosi alle istruzioni impartite.*

1. Incaricati come persone fisiche
2. La designazione degli incaricati via nomina è implicitamente obbligatoria, atteso che "solo" gli incaricati possono effettuare operazioni di trattamento
3. Anche il Responsabile può autonomamente nominare (firmare) un incaricato (molto utile per le esternalizzazioni)

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

TITOLARE, RESPONSABILE E INCARICATO…

E l'Amministratore di Sistema?
Fornitori come Co-processors

Una figura critica che assume un ruolo critico e/o fondamentale in relazione all'inquadramento nel sistema di deleghe.

Il più delle volte si tratta di un rapporto di esternalizzazione, quindi più critico negli scopi e nelle convenzioni reciproche

Ma la tecnologia può aiutare o condannare, dipende sempre dal MPS e dalle sue parti attuativa e operativa.

Nuovo Codice della Privacy
Decreto L.vo 196/03

SalvoReina

NOTIFICAZIONE INFORMATIVA CONSENSO

La contitolarità permette di condividerne l'impianto e unificare gli intenti tra le diverse sedi (ES. : stazioni ferroviarie)

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

La Notificazione al Garante
Cambiate le vecchie disposizioni

***Art. 38** (Modalità di notificazione)*

*2. La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di **sottoscrizione con firma digitale** e di conferma del **ricevimento della notificazione.***

*3. Il Garante favorisce la disponibilità del modello per **via telematica** e la notificazione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.*

Una prassi articolata e potenzialmente problematica per il Titolare del trattamento con aspetti, formali tecnologici e burocratici cui sono legate altre scadenze e adempimenti

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

La INFORMATIVA
Confermate le vecchie disposizioni

Art. 13 (Informativa)

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
a) le finalità e le modalità del trattamento cui sono destinati i dati;
- ***b) la natura obbligatoria o facoltativa del conferimento dei dati;***
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

Una corretta informativa è il presupposto iniziale della legittimità del trattamento. Di fatto chiunque intraprenda un sistema di tutela dei dati personali la ritiene implicitamente necessaria

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

CONSENSO (op-in / opt-out su WEB)

Art. 23 (Consenso)

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.
2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

Consenso dove associato alla informativa deve mantenere coerenza e può essere "***comunicato***" contestualmente.

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

CONSENSO

Come formalizzare correttamente a seconda degli interlocutori

Art. 23 (Consenso)

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.
4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

Attenzione alla potenziale perplessità: "***documento per iscritto***" e documento "***in forma scritta***"

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

Adempimenti idonei / essenziali

1. **Notificazione (ora Data Breach)**
2. **Informativa per l'interessato (sempre necessaria)**
3. **Richiesta di consenso, correlata all'informativa**

Un tavolino a tre gambe che presenta la immagine della organizzazione all'esterno.

Nuovo Codice della Privacy
Decreto L.vo 196/03

SalvoReina

LE MISURE MINIME DI SICUREZZA OGGI IDONEE E SOSTENIBILI

L'elaborazione di un quadro di principi e di regole rivolto a segnare il raccordo fra le dinamiche tecnologiche e la tutela dei diritti fondamentali della persona costituisce il fattore basilare per ogni ciclo di sviluppo economico-sociale.

Nella riforma GDPR

MISURE ADEGUATE

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza
Non esistono più !

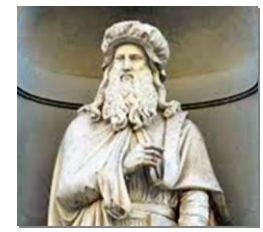
Trattamento dei dati personali "sensibili" con elaboratori in rete

- **Quanto previsto alla lettera B**
- **Accesso autorizzato singolarmente o per gruppo di lavoro**
- **Documento programmatico della sicurezza deve contenere un Disciplinare Interno**
- **Amministratori di Sistema competenti, anche esterni ma comunque corresponsabili !**
- **Provv. GU 45 Feb 2009**

DPS eluso da Monti adottato comunque nella realtà

Nuovo Codice della Privacy

In sede di ispezione ciò che premia è la sostanzialità e la concretezza di una misura



Misure Adeguate sono diventate Idonee !

La radice etimologica enfatizza il fatto che non esistono soluzioni standard ed ognuno può ideare soluzioni proprie, purchè concrete, funzionali ed efficaci.

Nuovo Codice della Privacy
Decreto Lg.vo 196/03

SalvoReina

Misure Idonee/adeguate di Sicurezza

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

SalvoReina

Misure Idonee di Sicurezza
UNO SGUARDO MIRATO ALL'ALLEGATO B

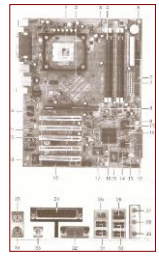
AUTENTICAZIONE:
si intende una procedura automatica che consenta di identificare l'utente che richiede di accedere al Sistema Informativo
Solitamente si associa un identificativo pubblico e una password segreta, ma sono ammesse credenziali biometriche, *token* o una combinazione di essi
Le credenziali 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

cosa chiedere agli informatici : AUTENTICAZIONE

Manuale del Sistema Informativo : **POST e BIOS setup**



Non trascuriamo misure elementari : la coerenza è una stima Della serietà professionale

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

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

Spieghiamo la PROFILAZIONE!

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

SalvoReina

Misure Minime di Sicurezza

ALL'ALLEGATO B (vediamo avanti dettaglio nella Sezione)

DOCUMENTO PROGRAMMATICO DI SICUREZZA

Non più 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 (DLg Monti Semplificazione)
- 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

SalvoReina

Misure Idonee 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

La documentazione cartacea del Sistema Privacy (ex DPS) è necessaria perché essa stessa è Misura Idonea di Sicurezza

Nuovo Codice della Privacy

cosa chiedere agli informatici

SalvoReina

Esempi semplici : Misure irrinunciabili e ovvie

ANTI VIRUS

- Sempre e comunque, almeno su tutti i client

Firewall

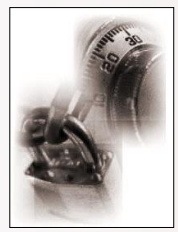
- Se si ha una connessione permanente (adsl) è opportuno inserire un firewall fisico a valle del router
- Su un client può essere sufficiente un *Personal firewall*

Sistemi Windows 95/98/XP

- 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

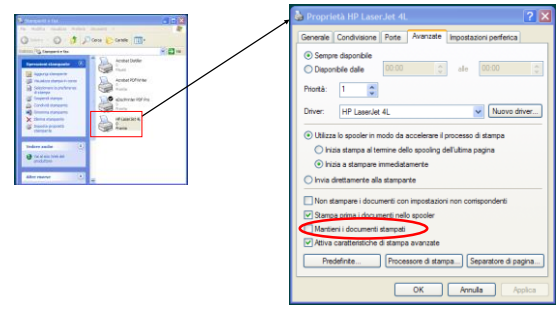


Uno occasione aziendale da sfruttare : GPO sui Servers (LDAP/AD)

Nuovo Codice della Privacy

cosa chiedere agli informatici : AUTORIZZAZIONE

Manuale del Sistema Informativo : attenzione allo spooler di stampa



Misure elementari possono preservare da sanzioni in sede di ispezione La coerenza minimale è una stima della serietà aziendale

Nuovo Codice della Privacy

cosa chiedere agli informatici

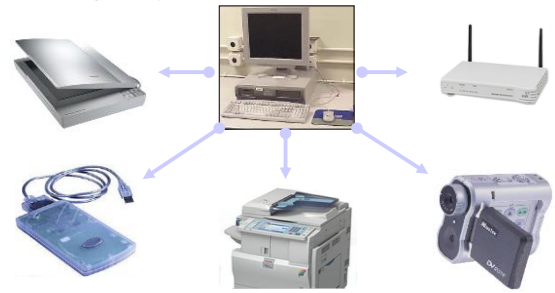
Manuale del Sistema Informativo : **spooler di stampa**

Perché pagare un hacker se basta consultare le informazioni
Se le hai stampate sono certamente importanti!

Nuovo Codice della Privacy

cosa chiedere agli informatici : LEAKs PERIMETRALI

Manuale del Sistema Informativo : **USB, PRT multifunzioni e dispositivi esterni di acquisizione, Access Controls**



Non trascuriamo misure elementari : la coerenza è una stima della serietà professionale

Privacy : **nuovo paradigma del futuro**

salvo.reina@realitynet.it

Unificazione Privacy e IT Security

DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

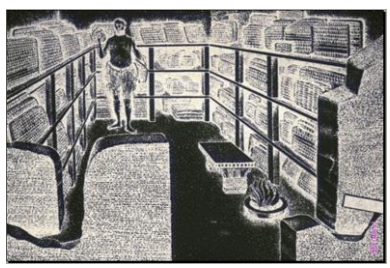
L'epica di un falso problema !
Il DPS diventa il MSP

e fino ad oggi come avete fatto ?

General **D**ata **P**rotection **R**egulation

Sistema Qualità e Sicurezza orientato alla gestione del rischio (Reg. 679/2016)

Nuovo Codice della Privacy



Procedure nell'antichità… perché non oggi?

Masterplan implementativo : NON interventi Ex Post

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

DPS – di fatto esiste sempre anche se non si chiama cosi !

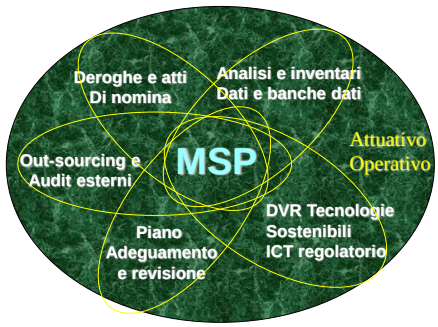
Oggi Manuale del Sistema Privacy (MSP)

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

DPS o MSP che sia rappresenta un vantaggio semplificativo di gestione

Per il Supervisore Europeo del Data Protection esitono gli **STATEMENTS**

Nuovo Codice della Privacy



NON ESISTE UN MANUALE CARTACEO PER TUTTI

SalvoReina

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

COME RENDERE CREDIBILE IL MSP

Ecco gli Statements !

Attuativo

Dichiarazione transattiva
Deleghe e Nomine
Valutazione dei rischi
Invetari e classificatori
Scadenziari (Es Formazione)

Operativo

PIA – privacy Impact Analysis
Piano di adeguamento (PA196)
Procedure e prassi
Istruzioni operative
Manuale Sistema Informativo (MSI196)
Disciplinare Interno

ATTENZIONE : Analisi dei Rischi preventiva !

Non solo carta…

SalvoReina

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

DOCUMENTAZIONI DI FRONTIERA

BRIDGING LAWS & REGULATION

DVR Dlg81/08

Documento di valutazione dei rischi DVR

DVR Dlg231/01

Integrazione DPO/ADS in ODV

DM 155 Legge Pisanu

Misure anti terrorismo (DI196)
Data retention
Mis-classification

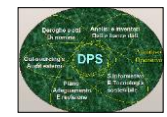
Manuale Sistema Informativo (MSI196)

Non solo carta…

SalvoReina

Nuovo Codice della Privacy

Decreto Lg.vo 196/03



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!

SalvoReina

Nuovo Codice della Privacy

Decreto Lg.vo 196/03

Tipologie credibili di sicurezza

Descritte sia quelle già adottate che in predicato se . richieste per migliorare il livello di protezione sulla base Delle attribuzioni di finalità dei trattamenti

CLASSI DI MISURE nel MSP

- FISICHE (antiintrusione, antiincendio, continuità 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

Approccio alle ISO9001 : Descrivere ciò che viene fatto e non ciò che "si dovrebbe fare"

SalvoReina

Nuovo Codice della Privacy

I CRITERI DI *DISASTER RECOVERY*

Dove nesessario adottare sito freddo: sicurezza alter loco

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)*

Approccio alle ISO27001 : Ricordare il criterio di sostenibilità per le Piccole e Micro aziende!

SalvoReina

Nuovo Codice della Privacy

SalvoReina

LA FORMAZIONE COME ADEMPIMENTO

Nel GDPR
Va diversificata per figura !

La consapevolezza e la collaborazione del personale sono critici per il successo e la funzionalità di ogni piano di sicurezza
Educare e istruire gli utenti è indispensabile (*oltre che necessario !*)

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

Privacy : un nuovo paradigma
NOVITA' DEL REGOLAMENTO EUROPEO

Come si fa la formazione : livelli di ruolo

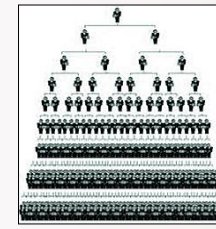
(accountability, statements introdotti nella privacy UE)

a) Proprietà

b) ADS

c) Incaricati

d) Esternalizzazioni
(Resp., Service, HW ecc)



SR

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 **estensione delle 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 (SLA e PLA)***
- ***Modalità per la verifica dell'operato del fornitore (ISO90xx:20xx)***
- ***Privative Clauses o BCR per forniture ICT***

Se non funziona, chi se ne occupa e chi paga ?

DISCIPLINARE INTERNO CONFORME AL PROVVEDIMENTO SUGLI ADS / DPO

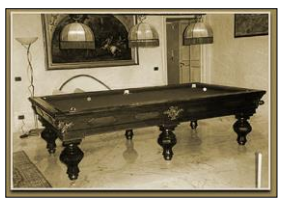
TDT dimostrare competenza ADS/DPO (contratto)
Disciplinare tecnico sul campo…
Protezione prese a muro e hub
Disattivazione device di bootstrap
Protezione spool di stampa e salva schermo
Tracciamento dichiarato mailer di posta e web agli incaricati
Dispositivi di acquisizione esterni
Cifratura questa sconosciuta e copie di sicurezza
Storicizzazione e alter sito

MISURE DI CONTROLLO PER GLI AMMINISTRATORI DI SISTEMA
Documenti di Due Diligence (Provvedimento Generale del 27 Novembre 2008)
PRONUNCIAMENTO 14 GEN 2009 G.U. N. 45 del 24 Febbraio 2009

Non sono gli imprenditori che rispondono delle incurie tecnologiche ma devono dimostrare di non scegliere a caso

Nuovo Codice della Privacy

Decreto L.vo 196/03



MSP è una partita di biliardo a dichiarazione…

General **D**ata **P**rotection **R**egulation

Sistema Qualità e Sicurezza basato su
Governance e Compliance
Senza **DPO** le organizzazioni rischiano

Nuovo Codice della Privacy

Decreto L.vo 196/03

SalvoReina

Evitare : gigantismo e nanismo, inutili
Coerenza e pertinenza nelle contitolarità !

SR

Privacy : un nuovo paradigma

Formazione e aggiornamento

a) Evoluzione della privacy

b) Istruttoria di compliance

c) Paradigmi futuri su CLOUD

d) Verifica Question Time

Nuovo Codice della Privacy

Decreto L.vo 196/03

SalvoReina

MSP, ADS, INFORMATIVA, CONSENSO, DISCIPLINARE TECNICO, CREDENZIALI INFORMATICHE

La contitolarità permette di condividerne l'impianto e unificare gli intenti tra le diverse sedi nelle stazioni

Privacy : ambiti problematici TUP verso GDPR

dalla conformità alla compliance

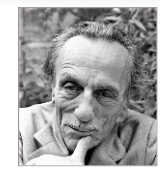
Riassumiamo prima dei requisiti di ***COMPLIANCE***

- Persone giuridiche e fisiche – criterio di proporzionalità e finalità
- Responsabilità e sanzioni – non più soglia ma a % del fatturato
- Formazione continua e somministrazione SOP – conformità vs compliance
- Deleghe e nomine verificate e verificabili : DPO o ADS
- Misure idonee e non solo minime – dal DPS al Privacy Governance
- OPT-IN / OPT-OUT – Informative/consensi via Portale
- Diritto all'oblio – cancellazione definitiva
- CLOUD e trattamenti IT (anonimizzazione, conservaz. Sostitutiva, dematerializzazione)
- Delocalizzazione e BYOD : ibrido dispositivi privati-aziendali
- Contrattualistiche : SLA e accordi di settore – trattamenti con estero
- Disciplinare e Policy condivisa con incaricati – superate RSU e DPL
- Carta di identità elettronica – Misure addizionali per ADS
- Inclusione digitale – Agenda Digitale 2.0
- Misure di backup alter loco : Sito freddo e terzializzazioni IT
- Misure anti frode : furti di identità e preservazione contraffazioni
- Ordini professionali e accordi di settore (AGICOM, ANIA ecc..)

Cosa non fare ?

Ha da passà a' nuttata …

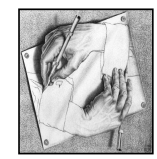
Le Direzioni Risorse Umane sono di fronte ad un'importante fase di cambiamento. Sono chiamate a raggiungere obiettivi in apparente contraddizione: *ottimizzare i costi, orientare le persone agli obiettivi aziendali, adempiere ad una normativa in continua evoluzione e che prevede sanzioni sempre più aspre in tema di privacy e sicurezza.*



Cosa fare ?

EDUCAZIONE E ATTITUDINE PER AUTOCONTROLLO E AUTOREGOLAMENTAZIONE

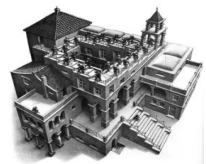
Un atteggiamento pro-attivo è sempre più conveniente. Sfruttare la privacy come un opportunità di un maggiore empowerment della funzione nel raggiungimento degli obiettivi di business ha un'importanza sempre crescente e la Direzione Risorse Umane deve riuscire a misurare, valutare e monitorare i processi.



Come approcciare le notivà ?

Approccio ad un nuovo paradigma non a un vecchio paradosso …

Privacy by desing
Privacy by default



Non c'è Amministrazione Digitale 2.0 senza Privacy

Comunicazioni On-line, Cookies (Dlg 69/2012 Art.122), violazione dato personale Provv. "Data Breach" (Art. 3, 32, 132, 162-ter Codice privacy), pregiudizio violazione a terzi (150K€ non più del 5% fatturato). Conservazione dati di traffico (Dlg 109/2008 modalità) e Codice Privacy per misure conservazione

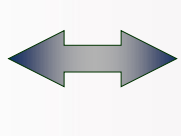
Privacy : New Paradigm of Readiness

Dalla ispezione … all' …. *Audit*
Dalla conformità … alla … *Compliance* !

Emancipare dalla logica della casalinga alla donna manager !

Privacy : New Paradigm of Readiness

… essenzialmente risolvere i conflitti …



ICT : Cloud, network sec, Malware, BYOD,, data recovery, business continutity

MSP : manuale, Disciplinare interno, diritti interessato, formazione obbligatoria

Notificazione : rapporti con Autorità, obblighi istituzionalizzati

Legal : Audit, piani 231, video sorveglianza, statuto lavoratori, Digital divide, pro-active operator control

Forniture : HW/SW, servizi SLA e Clausole contratti,

Vision : business, acquisti, personale, policies e regulation

Per non confondere sforzi con risultati … check-list

Privacy : New Paradigm of Readiness

Costo / beneficio

La filosofia di consenso alle risorse umane

Infondere i concetti funzionali della *compliance*:

La sicurezza Non è Non fare le cose !

E' stabilire Prima come, dove e da chi vanno fatte

Ciclo DEMING :Stimare la qualità nera !

Privacy : New Paradigm of Readiness

Concetti funzionali della *compliance*:

condividere

a) **Le informazioni giuste**
(Proporzionalità trattamenti con la finalità)

b) **Al momento giusto**
(Pianificazione e schedulazione Es. formazione)

c) **Con le persone giuste**
(Accountability legata segregazione mansionari)

Data Protection : il DPO assiste l'azienda **affiancando e convincendo** gli informatici

IT READINESS cruciale !

Esistono solo due tipi di utenti:

Quelli che hanno un PC infettatto…
e…
Quelli che non sanno di avere un PC infettato

enisa

Maggiore fonte di perdità economica !

Privacy : un nuovo paradigma
NOVITA' DEL REGOLAMENTO EUROPEO

Effetto domino :
visione miope del danno !

a) Interruzione di servizio

b) Manutenzione straordinaria

c) Loss of ROI

d) Capitals Leaks

e) Information dissemination

Perché AUDIT IT

È cruciale : BOTNET

Contratto di Intrusione amicale e implicito consulenza DPO

A chi si chiede perché …

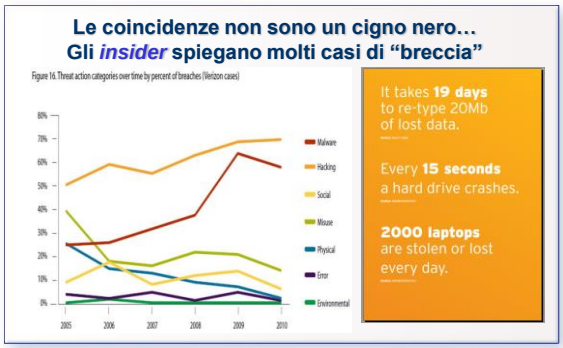
Il crimine informatico
Basso rischio, opportunità e alto profitto
…
E' più sicuro !

Anche il basista che agisce dove i Sistemi Informativi non sono curati da un ADS per la privacy
…
E' più sicuro !

Fiorente mercato di credenziali per il social engineering … molto spesso parenti, figli smaliziati o affiliati di cosche (provincia…)

Source: Chat Interview with the Dream Coders Team, the developers of MPack
http://www.robertlemos.com/2007/07/23/mpack-interview-chat-sessions-posted/

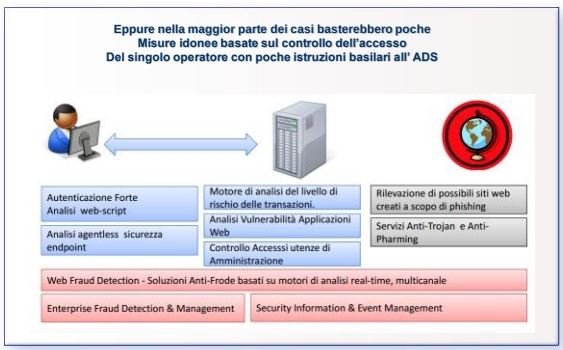
Come succedono le cose?



Fonte Verizon- 2011 Data Breach

Gli Europei come fanno ?

COME DECIDERE : Mandatoria la figura del DPO



FORMAZIONE FIGURE PRIVACY : una figura educativa !

Inelluttabile, irrinunciabile ?

Privacy : un nuovo paradigma
NOVITA' DEL REGOLAMENTO EUROPEO

Ecco perché usiamo la Steganografia !

COME DECIDERE : trucchi pratici del DPO

Competenze DPO

Normativa privacy nelle attività aziendali DP

Linee Guida per l'audit dei Sistemi di gestione (ISO 19011:2012)
Sistemi di gestione della qualità (ISO 9001:2015)
Sistemi di gestione Sicurezza infrastrutture IT (ISO 27001:2014)
Sistemi di Gestione Servizi IT (ISO 20000:2010)
Princìpi di Risk management (ISO 31000:2010)
Princìpi di Business Continuity (ISO 22313:2015)

COME DECIDERE : trucchi pratici del DPO

Formazione educazione alla professionalità
Per difendere sia la persona che l'azienda

Anche nello stile di piccole cose !

Poche regole basilari di abitudini davanti al PC

- *Impostare una password su smartphone, tablet e portatile*
- *Creare un avviso su Google con il nostro nome*
- *Disconnettere sessioni dei servizi che usiamo*
- *Non dare la propria email a tutti*
- *Criptare i dati sul proprio computer*
- *Abilitare la verifica in due passaggi (ES.Gmail)*
- *Pagare in contanti o con monete elettroniche*
- *Aggiornamenti su Facebook visibili soltanto agli amici*
- *Pulire la cronologia di navigazione del browser*
- *Mascherare il proprio indirizzo IP*

Aree-Attività critiche : TdT e ADS

Cambi di paradigma

Esempi :

- *Elettricità vs fuoco*
- *Motore scoppio vs cavallo*
- *Aero vs treno*
- *Radio vs colombi viaggiatori*
- *Televisione vs radio*
- *Internet vs poste*
- *Dematerializzazione vs carta*
- *Anonimizzazione vs dato personale*
- *Deanonimizzazione vs privacy*
- *Delocalisation vs posizione fisica*
- *Network vs area locale*
- *Distributed extranet vs private office*
- *Corporate networks vs Clouds*
- *Persona digitale vs individuo analog*

Ogni salto dimensionale tecnologico implica modifiche di obblighi normativi, requisiti tecnologici e di prassi e costumi di comportamento

Un cambiamento di prospettiva che ci insegue nello specchietto retrovisore e al cui sopraggiungere non ci si può sottrarre

COME DECIDERE : Mandatoria la figura del DPO

Perché conviene il supporto di un integratore !

PROTEZIONE DEI DATI PERSONALI (PRIVACY)
Assistenza ad ogni adempimento previsto da leggi e provvedimenti in materia di privacy.

ANALISI DEI RISCHI
Finalizzata alla IT Governance aziendale ed agli adempimenti obbligatori, quali:
- Art.31 d.lg 196/2003 e DPS

BUSINESS CONTINUITY
Assistenza alla compilazione del Piano di Continuità per i processi critici

PIANI DI SICUREZZA E ICT AUDITING
Compilazione di *Policy* di sicurezza aziendali. sistema di controllo delle principali aree IT

Cosa può fare un DPO rispetto alla tradizionale CDA

Intermediazione di metodi e linguaggi trasversalmente al business management

Interfaccia tecnico-regolatoria con l ' IT (logs, email, data retension ecc)

COME DECIDERE : Mandatoria la figura del DPO

Provvedimento male implementato ma cogente degli ADS
Nel trattamento di informazioni sensibili digitali

- Uso combinato di almeno due tecnologie di autenticazione
- Separazione fra funzioni di assegnazione delle credenziali e gestione tecnica di sistemi e database
- Conservazione separata per finalità
- Server con i dati conservati a fini di accertamento/repressione reati, in locali ad accesso selettivo e controllato
- Formazione periodica degli incaricati
- Tracciatura degli accessi (audit log)
- Audit interno – Report periodici
- Documentazione dell'ingegneria del sw

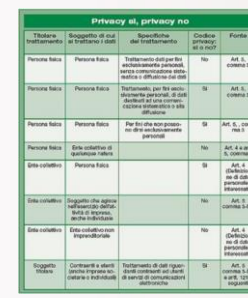
Cosa può fare un DPO : guida gli informatici nella formalizzazione documentale e sostanziale degli adempimenti

COME DECIDERE : Mandatoria la figura del DPO

Persona fisica
e
persona giuridica !

Cosa un DPO adiuva
Il tradizionale CDA

Trucchi del mestiere per identificare la struttura gerarchica e le responsabilità nel modo più conservativo per tutelare le persone fisiche nel caso di controversie o contenziosi



COME DECIDERE : Mandatoria la figura del DPO

Contitolarità

Economizzazione risorse
Condivizione del documentale DPS
Condivisione policy degli ADS
Centralizzazione del dato informatico
Centralizzazione delle prassi di sicurezza
Consultazione delocalizzata a norma
Data base "di cortile" monitorato
Riduzione delle comunicazioni verbali
Pubblicazione MSP WEB intranet

Cosa può fare un DPO rispetto alla tradizionale CDA

Strumento sottovalutato anche dagli avvocati : trucchi del mestiere per sfruttare la legge nei casi corporativi e distribuire gli oneri (Filiali, multinazionali, consorzi)

COME DECIDERE : Mandatoria la figura del DPO

Notificazione e Preliminar Check

Cosa può fare un DPO rispetto alla tradizionale CDA

Svolgere la prassi
Istruttoria compilativa
Scelte appropriate per business
Scongiurare errori di incompetenza
Pratica presso "**Intermediari**"

Se fatta bene rappresenta l'indice di un buon MSP

Ricordiamo che la omessa o errata notificazione per il 2010-2011 è stata presente il 32 % dei procedimenti sanzionatori.

Dal Gennaio 2013 è praticamente obbligatoria per qualunque trattamento (poche eccezioni nella PA) e addirittura sono state introdotte "Preliminar Check". Siccome via web allora la fa il sistemista !

Nessuna area ICT è indenne alla Preliminar Check UE ...

Notificazione e Preliminar Check

Anche la Sicurezza Nazionale negli USA ha fatto un passo indietro E ha sfumato !!!

Lobby della IAPP !

A fiumicino sostituiti 16 body scanner **Preliminar Check** Autorità !

COME DECIDERE : Mandatoria la figura del DPO

Adiuvare il legale della società

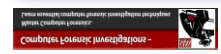
Incident Group Response

Contenuti proprietari : cugino compiacente porta all'esterno documenti

Litigation : Ricorso per mobbing ingiustificato

Post firing: vendette dopo licenziamento anche non a scopo speculativo

Cross competition : remore e conflitti con altri dipendenti



Riflessione : quando i dipendenti si rivalgono con una causa di "Digital Forensic" ?

COME DECIDERE : Mandatoria la figura del DPO

Decisione rischiose e attività critiche per :

eMails : controllo pro-attivo. Risponditore automatico, forward aziendale, CC/BCC

Routers/Firewall : discriminazioni, settings filtro navigazione

Navigazione : Intranet/Extranet, VPN corporativi, Provvedimenti WEB es. **Cookies** !

Deleghe e nomine : corrette attribuzioni, affiancamento, policy sostanziale, scelta dell' ADS compete solo il TDT

Disciplinare interno : divulgato, validato in formazione, verificato periodicamente

Aree-Attività critiche : TdT e ADS

VS e statuto lavoratori

Digitalizzazione documenti

SOP/POS servizio protezione dati

Tracciamento e-mail e navigazione

Aree-Attività critiche : TdT e ADS

Anonimizzazione
Deanonimizzazione !

Ambiti :

- *Assicurazioni*
- *Corporazioni bancarie*
- *Sanità e diagnostiche*
- *Genetiche a fingerprint digitale*
- *Profilazioni abitudini*
- *Libero movimento / pensiero*
- *Privacy individuo-istituzioni*
- *Privacy individuo-commercio*
- *Monitoraggio sicurezza*
- *Banche dati*
- *Centrali di rischio*
- *Investigazioni legali/private*
- *Obblighi verso dipendenti*

Oblio e right to be forgotten

Ora sono le università che strette dalla crisi rivendono la propria abilità e conoscenza informatica per agire come cybercrime !

Il titolare del Trattamento ha l'obbligo di delega per l' A.D.S. !
Dove necessario un DBA e un System Manager separati per non incorrere in conflitti di interesse

Aree-Attività critiche : TdT e ADS

Archiviazione sostitutiva !

Di fatto :

gestire l'intero ciclo di vita del documento certificandone il contenuto tramite apposizione di firma digitale e marca temporale, che rendono un documento non modificabile, opponibile a terzi e non deteriorabile, quindi disponibile nel tempo in tutta la sua integrità ed autenticità

Per DEMATERIALIZZARE
Un ADS non basta, occorre un DBA distinto che riferisce al TdT

Oblio e right to be forgotten

Conservare digitalmente

significa quindi sostituire i documenti cartacei, che per legge si è tenuti a preservare, con l'equivalente documento informatico.

Avete preservato SQL-INJECTION ?

Il titolare del Trattamento ha l'obbligo di delega per l' A.D.S. !
Dove necessario un DBA e un System Manager separati per non incorrere in conflitti di interesse. Chi controlla il controllore ?

Privacy : un nuovo paradigma
NOVITA' DEL REGOLAMENTO EUROPEO

Archiviazione su dispositivi *edge*: inferno o paradiso?

Con l'avvento degli slot SD integrati direttamente nelle telecamere IP, il concetto di registrazione su dispositivi "**edge**" ha fatto recentemente la sua comparsa.

VIGILANTES o Ag. Security hanno...

... FIRMATO o solo FILMATO ?

IndigoVision

29/01/2013, Alex Swanson, BSc, MSc, IndigoVision Head of Engineering)

Aree-Attività critiche : TdT e ADS

Archiviazione sostitutiva !

Altra mitologia da sfatare

PA vs privato !

Perché è un errore omologare e sottovalutare, o peggio, ignorare gli obblighi della PA ?

Il problema lo deve gestire chi partecipa l'appalto e lavora per la PA !

L'esempio del DISASTER Recovery

La Legge 231 rende mandatorie le misure di Disater Recovery per tutte le attività degli uffici pubblici. Addirittura in modo vincolante nei casi di Servizi OnLine

Il titolare del Trattamento ha l'obbligo di delega per l' A.D.S. !
Un semplice documento di scambio con il Fornitore Esterno per essere inattaccabili

Aree-Attività critiche : TdT e ADS

Security: VIRTUALIZZAZIONE

Accountability e Statements

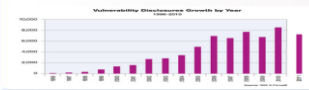
a) **Multiplatform**
b) **Delocalisation,**
c) **Backup,**
d) **training machine,**
e) **Offuscamento**

B_Sync
Sito freddo - caldo

security

Data Protection : migliore risposta

WI-FI – un problema anche per gli hackers quello del MITM



Attacks always get better;they never get worse. (NSA)

Mallory is always with your wife !

NATIONAL SECURITY AGENCY

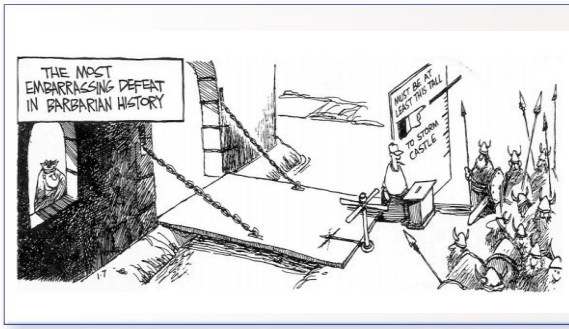
Data Protection : AUDIT unica alternativa

Le regole del Gioco non le decidiamo… La Data Protection aiuta a non subirle (ISACA)

A cosa serve DPO : aggiornamento continuo

- Uso combinato di almeno due tecnologie di autenticazione
- Separazione fra funzioni di assegnazione delle credenziali e gestione tecnica di sistemi e database
- Conservazione separata per finalità
- Server con i dati conservati a fini di accertamento/repressione reati, in locali ad accesso selettivo e controllato
- Formazione periodica degli incaricati
- Tracciatura degli accessi (audit log)
- Audit interno – Report periodici
- Documentazione dell'ingegneria del sw

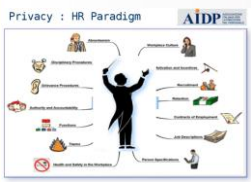
La Resilienza… Paradigma globale DP



Firewalls and Internet Security - W.R.Cheswick & S.M.Bellovin - 1st Ed 1994
cover illustration by Wiley Miller

Dalla Sicurezza alla Resilienza…

Integrazione
Total Quality Management
Non basta la carta.
Il Data Protection traversa sostanzialmente le funzioni aziendali!



Fonte:
Booz&Company, 2011

La vulnerabilità e inversamente proporzionale al successo di business …

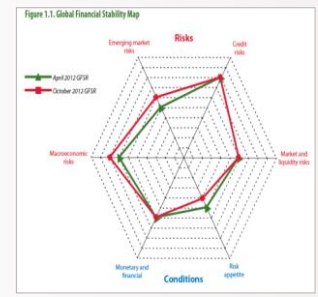
Se non siamo resilienti ?

ICT vincola lo sviluppo globale

Le analisi macro-economiche dei Fattori di rischio

Vulnerabilità di Identità del consumo nel mondo

ADS intelligente
Adotta IDS/IPS



Source:
GFSR (Oct 2012)
www.imf.org

FOLLOW INSEAD KNOWLEDGE ON OUR Forbes

La vulnerabilità e inversamente proporzionale al successo di business …

40 % Attacchi costano 4 giorni di stop !

90 % degli attacchi … mancate competenze, errate configurazioni HW e SW

Nel 2011 in Italia 55 miliardi di USD di danno 86 Miliardi nel 2012

Pubblico e Privato

EU strategy on cyber-defence

Società del rischio tecnologico globale…
Una questione che puzza di UMANO
SUCCEDE SEMPRE AGLI ALTRI!

Rischio digitale senza confine con probabilità di *eventi critici* per il fattore umano

Con il tempo, ciò che è impossibile diventa possibile, ciò che possibile poco probabile, ciò che è improbabile … certezza !

La Place

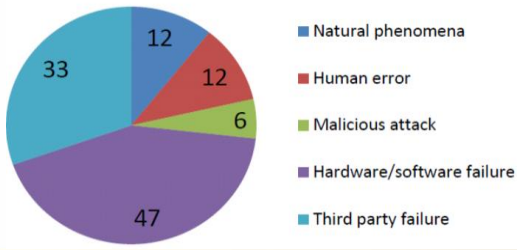
Considerare la sicurezza, confidenzialità e privacy ICT:

- in termini non strettamente digitali ma globali (fisici-logici-organizzativi)
- non un adempimento tecnico-burocratico, ma un valore organizzativo
- non un costo da tagliare, ma un investimento strategico

enisa

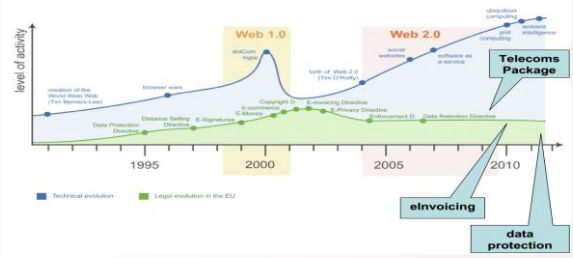
Società del richio tecnologico globale…

Una questione legata al fattore umano e SLA fornitori HW/SW



Source:
Annual Incident Report 2011 (Oct 2012)
www.enisa.europa.eu

Obblighi regolatori con evoluzione ICT … **WEB**



Non fate sul sito WEB gli errori risolti dentro casa !!!

Fonte: Legal analysis of a Single Market for an Information Society EU Commission, 2009, con aggiunte

Holistic approach compliance ICT …

Una questione di risoluzione e dettaglio !

$R = f(I, T, V, C)$

Non occorre una valutazione analitica matematica del calcolo del rischio

Un censimento sistematico delle funzioni e del loro contorno è sufficiente per un Sistema Qualità e Sicurezza

Ho visto la Madonna !

Assets, organigramma, DVR/PIA, level acceptability and sustainability

CL0UD : UNA DIAPOSITIVA… UNA STORIA !

I vantaggi sono chiari parliamo dei problemi di contrattualità

Public, Private and Hybrid

Localisation data transfer
Reponsabilities identification
Impacts on consumers and actors's roles
Infrastructure Player e SLA – Provider, Broker, consumer

Chi è il TDT e il proprietario ?

SaaS – Service as Service
PasS – Platform as Service
IasS – Infrastructure as Service

cloud security alliance Italy Chapter

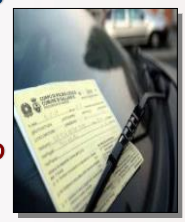
Portabilità, governance,sub fornitura, e falsa resilienza, Team di risposta incidenti, Standard Contractual Clauses

Un DPO tutela la azienda sia nel rapporto di fornitura che nelle configurazioni dei servizi.

Data Protection : un nuovo paradigma

Formazione e aggiornamento

a) Evoluzione della privacy
b) Istruttoria di compliance
c) **Paradigmi futuri su CLOUD**
d) Verifica Question Time



Perché fare le cose sotto regime terroristico ?

Qualche nozione prima di pagare …

Dal 38° al 42° posto capacità di utilizzo ICT
Global Information Technology Report 2007-2008" del World Economic Forum (Wef)

Dal 42° al 48° posto capacità di utilizzo ICT
Global Information Technology Report 2009-2010" del World Economic Forum (Wef)

Banda larga e U-WI-FI
Servizi ICT convenzionali
mBanking e eBanking
E-waste e data retention
Cyber-security e Privacy
Copertura infrastrutture ICT
Big data & Cloud future
Virtualisation & dematerialisation

DIGITAL DIVIDE

FOLLOW INSEAD KNOWLEDGE ON OUR Forbes

Voi direte, in Italia abbiamo la creatività !

Secondo Assintel solo il Data Protection È la **chiave** per la NUOVA IT italiana

Competenze certificate per traversare DLg196/03, Dlg231/01, Safety, Security e Qualità riducendo costi, risorse e migliorando integrazione

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

TOTAL RANK	COUNTRY	TECHNOLOGY	TALENT	TOLERANCE	GLOBAL CREATIVITY INDEX
1	Sweden	5	2	7	0.923
2	United States	3	6	8	0.902
3	Finland	1	1	19	0.894
4	Denmark	7	4	14	0.878
5	Australia	15	7	5	0.870
6	New Zealand	19	5	4	0.866
7	Canada	11	17	1	0.862
7	Norway	12	6	11	0.862
9	Singapore	10	3	17	0.858
10	Netherlands	17	11	3	0.854
11	Belgium	16	12	13	0.813
12	Ireland	20	21	2	0.805
13	United Kingdom	18	19	10	0.789
14	Switzerland	6	22	20	0.785
15	France	14	23	16	0.764
15	Germany	9	28	18	0.764
17	Spain	24	28	6	0.744
18	Taiwan	–	32	21	0.737
19	Italy	26	18	23	0.707
20	Hong Kong	22	37	12	0.691
21	Austria	13	30	35	0.663
22	Greece	38	9	37	0.638
22	Slovenia	23	10	51	0.638
24	Serbia	28	35	27	0.614
24	Israel	4	20	66	0.614

MARTIN Prosperity Institute

Ponemon INSTITUTE

Privacy : Controllo e sistema sanzionatorio

Chi fa le ispezioni e i loro numeri

Cosa è il GAT ?

Nucleo della Guardia di Finanza elettivamente dedicato alle ispezioni in ambito Privacy.

Rapporto del Garante (*2010-11*)

- **Ispezioni** : 230 ispezioni, 181 procedimenti sanzionatori, 13 violazioni penali
- **Omesse** : informativa, notificazione, misure idonee, nomine/deleghe ADS
- **Mancati adempimenti** : provvedimenti, adeguamenti comunque cogenti
- **Ambiti** : investigazioni, assicurazioni, sanità, profilazione CentRischio, telemarketing
- **Comminazioni** : 3 milioni 234 mila € in 15 mesi

Privacy : Controllo e sistema sanzionatorio

Tipi di controlli

Le ispezioni possono avere tre tipologie

1. Casuali
2. Sistematiche /concordate
3. Su segnalazione / denuncia

Il tipo di verifica condiziona le regole di ingaggio per gli incaricati, per i responsabili e per il Titolare del trattamento. **Ricordarsi della Preliminary Check per dati sensibili !**

La conoscenza delle regole influisce sulla probabilità / entità della sanzione !

Privacy : Controllo e sistema sanzionatorio

Due check list veloci : cosa controllano i controllori ?

- ADOTTARE MISURE MINIME DI SICUREZZA All. tecnico B
- FORNIRE INFORMATIVE ART. 13 (INTERNE ED ESTERNE)
- NOMINARE INCARICATI (art. 30) E RESPONSABILI (art. 29)
- REGOLE SCRITTE PER TRATTAMENTI CARTACEI
- REVISIONE ANNUALE DEI DOCUMENTI
- ISTRUZIONI AGLI INCARICATI

- Autorizzazioni Generali
- Deliberazione n. 53 Linee Guida dati personali di lavoratori 23 novembre 2006
- Provv. Lavoro: linee guida per posta elettronica e internet - 1 marzo 2007
- Provv. su Amministratori di Sistema 27 novembre 2008
- Provv. su videosorveglianza 08 aprile 2010

La conoscenza delle regole di ingaggio influisce sulla entità della sanzione !

Privacy : Controllo e sistema sanzionatorio

Attualmente parliamo di

Fascie classificate con il Decreto semplificazioni

Da **20.000** a **120.000** euro

In caso di maggiore rilevanza per uno o più interessati da **40.000** a **240.000** euro

Garante può quadruplicare a seconda delle condizioni economiche del contravventore

Codice Penale per maggiore nocumento provato inasprico fino a 3 anni reclusione

Regolamento Europeo → **Fino al 2% del fatturato globale della organizzazione ! Neppure le multinazionali possono far finta di nulla !**

Privacy : Controllo e sistema sanzionatorio

Esempio : l'avvocato replica con una memoria difensiva **(delle BCR o PC avrebbero risolto !)**

La prossima volta la Società IT farà bene a cooperare

Da **20.000** a 75.**000** euro

L'aggravante considerata è stata la mancata replica

1. Agli interessati (fax indesiderati "*unsolicited practise*"),
2. Alla autorità (richiesta di chiarimenti),
3. Permutazione del minimo edittale (inadeguato testo difensivo)

Regolamento Europeo → **quanto previsto dall'articolo 157 del Codice privacy (sanzione amministrativa)**

In conclusione : nuova filosofia per tutelarsi

Non necessariamente dobbiamo essere geni che conoscono la relatività !

Il salto quantico occorre
- Commitment proprietà
- una delega forte
- un DPO

E atterrate in sicurezza…

Privacy : un nuovo paradigma

Formazione e aggiornamento

a) Evoluzione della privacy
b) Istruttoria di compliance
c) Paradigmi futuri su CLOUD
d) Verifica Question Time

Profilo professionale

Excursus accademico e competenze

- Ricercatore e docente universitario
- Biotecnologia e QA biomedicale
- Total Quality Manamentt - Auditor
- Data protection officer
- Privacy & Safety Blogger
- Company ICT Security advisory

tiro al piattello !

Certificazioni

Accreditamenti e affiliazioni

- ISO 27001:2009
- AM ISACA
- TÜV DPO (ISO 17024:2005)
- Ref. FEDERPRIVACY

Expertise & skills

- Integrator & Advisor on 231, Dlg191/07, Dlg81/08
- Data protection officer, CDA
- Privacy & Safety Advisor & Blogger

Verifica in aula