

GDPR/16/EU - Data Protection Era

La sicurezza nella gestione di dati e informazioni delle organizzazioni

GOVERNO RISCHIO COMPLIANCE

GRC e GDPR

IL MONDO FUTURO DELLA
Risk Data Management

UNIFICAZIONE
PRIVACY & SICUREZZA ICT

DAL DATO VS PRIVACY LIQUIDA E
PROTEZIONE DATI COSMICA



Data Protection : **paradigma futuro dei Dati**



Accortezze per il corsista

- a) Vibra call / cell. silenziato
- b) Ridondanza intenzionale
- c) Quali interruzioni possibili
- d) Annotazioni e discussione modulo
- e) Materiale corso su pendrive

Per non addormentarsi ...

concetti concentrici
nozioni applicabili
fissità verticali
sospensioni lacunose
memento incidentale



Data Protection & ICT Security

La sicurezza nella gestione di dati e informazioni nelle organizzazioni

GOVERNO RISCHIO COMPLIANCE

G.R.C. e GDPR

Percorso tematico

- 1. Ontogenesi e filogenesi del dato
- 2. Ciclo di vita ed evoluzione normativa
- 3. GDPR: rivoluzione di un paradigma
- 4. Instrumentazione e Readiness del GRC
- 5. Implementazione del Modello Aziendale
- 6. Validazione «moderata» delle acquisizioni



Data Protection : **CONOSCIAMOCI MEGLIO!**

indagine esplorativa, informale in ambito privato e PPAA.

Ruolo/funzione in azienda?

Estrazione studio/professionale:
ICT, management, legali o proprietà

Quanti tra ICT sono già ADS?

Quanti tra HR sono già ROT/ODV231?

Quanti del management sono ROT?

audience : quanti sono incaricati Sistema Privacy aziendale



Data Protection : **ESERCIZIO DI STILE**

HardWare <--- 01010001 --->>> SoftWare

TCP-IP MITM	MALWARE ANTIVIRUS Dockers
FIREWALL CMS	RANSOM'S WARE PLA SLA SLO
MODEM IoT	DB-SERVER
OSI OWASP	NO-SQL DB
BYOD RDP VOIP	USB-DRIVE
CLOUD SLA BIOS	SAS-Sata HD
CYBERSPACE	RJ-45/VPN
WEB 3.0 Portale	ROUTER
PLATFORM APP	WAN-LAN
ERP/CRM ZIP	RESILIENZA
Linux/Windows	DHCP-NAS RSA-SHA256-UTMs- BlockChain



Data Protection: futuro UNIFICATO di PRIVACY e IT-SECURITY
Basta ipocrisie tecnologiche-normative

PRIVACY

GDPR
Reg.
679/16

IT SECURITY

Non forma... più sostanza

DATA PROTECTION

Cambiamento non normativo ma economico e sociale perché i dati sono una materia prima!

Dato : status / trattamento / trasporto

DATA PROTECTION

Lo stesso dato cambia significato (informazione / comunicazione) secondo attività e contesto

Dato : status / trattamento / trasporto

DATA PROTECTION

Contesto Dato : statico - dinamico

Business continuity

disaster recovery

physical safety

Logical meassures

Confidentiality

Anti-intrusion

Non Repudiability

Perishability

Anti-corruption

G.R.C. : DATA AT REST <=> DATA IN MOTION

Prepararsi a conformare anche Per il FINE VITA !

DATA PROTECTION

Data Protection : ontogenesi e filogenesi della informazione

Informazione Aggiornamento Consapevolezza

a) Evoluzione Tecnologica dei dati

b) filogenesi delle Normative Privacy

c) Dalla Conformità alla Compliance

d) Dalla protezione alla Readiness

e) Orientamento Data Risk Management...

Per prepararsi al futuro ... capire il passato...

Data Protection : nuovo paradigma del futuro



PRESS RELEASE
EDP/2015/001
Brussels, Wednesday 22 January 2015

EDPS Strategy 2013-2014 for excellence in data protection by the EU institutions

JUSTICE

DATA PROTECTION

Opinions and recommendations

Una questione sovranazionale – Elaborazione giuridica ha seguito adeguandosi al progresso tecnologico

Trilogio UE : Parlamento, Commissione e Consiglio

Modello di GDPR

Identificare

Trattamenti, Dati Interessati, Destinatari, Responsabili, Almeno 8 rischi

Controllare / Formalizzare

PIA, Scenari, Principi e Policy, Azioni responsabili, Informazione e consenso, Autorizzazioni al trattamento

Erigare

Dati personali, Accesso, Rettifica, Oblio, Informativa e consenso, Trasparenza

Monitorare / Proteggere

Incidenti (Data Breach), Audit, Conformità

Commissione

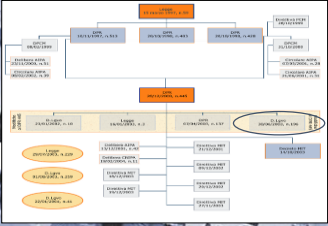
Parlamento

Consiglio

EDPB

Comitato: gruppo ex Art. 29 WP29 – Board ex Garante Garanti

GDPR Dal 1995 ...



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

Data Protection : nuovo paradigma del futuro
GDPR-EU e Reg.679/2016

Da Carta di Nizza (2000) al Trattato di Lisbona (2007). Da Parigi a Strasburgo, da Karlsruhe a Bruxelles fino a Shengen in Aja

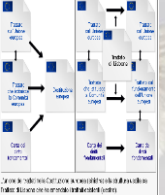
“diritto generale della personalità” legato Diritti fondamentali.

Processo di «Autonomizzazione» dagli USA

Privacy al momento attuale:
Legge Delega 25 ottobre 2017 n. 163 e 205 per armonizzare Regolamento con Codice Privacy entro 21 Maggio 2018

Persona elettronica corrispondente alla nostra identità digitale

Confidenzialità e riservatezza: un diritto non una virtù



Data Protection: **Non Come ma** Cosa
Persona e identità digitale

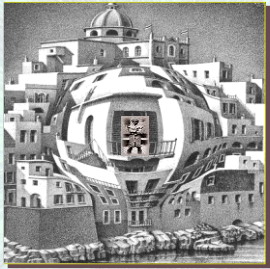
IT SERVICE COMPANIES

CRITICAL INFRASTRUCTURE

PUBLIC ADMINISTRATION AND PUBLIC SERVICE

Legislazione pensata per qualunque realtà di business

GDPR-EU e Reg.679/2016



Fuoco sulla persona... in che senso

SEFT Srl - 2018

3

GDPR-EU e Reg.679/2016



NON fuoco alla persona !

GDPR-EU e Reg.679/2016



ì MIEI DATI
SONO MIEI (?)

GDPR-EU e Reg.679/2016 in Azienda

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 / azienda* 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

Purtroppo non siamo Isopteri e l'azienda non è un termitaio

Privacy in azienda

Persona elettronica corrispondente alla nostra identità digitale

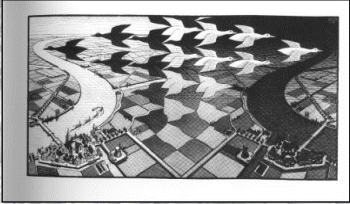
QUALE ???





Formazione del TRILOGO UE: Cultura aziendale e consapevole

GDPR-EU e Reg.679/2016



Due opposte libertà: libera circolazione dei dati tutela privacy

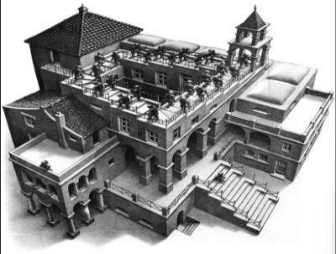
Una migrazione culturale evolutiva

GDPR-EU e Reg.679/2016



Se decide solo la forza, vince il più forte!
«Privacy by Design» + «Security by Design»

GDPR-EU e Reg.679/2016



LA SFIDA

Conciliare nuovi scenari degli sviluppi tecnologici e dei nuovi modelli di crescita sociale ed economica con la irrinunciabile e fondamentale esigenza di tutelare le persone fisiche. In ultima definizione, esseri umani

Paradosso o paradigma : individuo o azienda ?

Riforma della Data Protection



EDUCAZIONE AUTOCONTROLLO E AUTOREGOLAMENTAZIONE
INTERESSE CONGIUNTO DI IMPRENDITORE E LAVORATORE

Reg.679/16 sulla Data Protection

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



Reg.679/16 sulla Data Protection

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

Reg.679/16 sulla Data Protection

675/96 318/99 196/03

Detenzione Trattamento Comunicazione

11/2008
A.D.S.

2/2012
No DPS

Dlg5/2012
Viol. Telco

Dlg69/2012
Market/ISP

Reg.UE2014/EIDAS
Identità Digitale

Reg.UE/680/16
Contrasto
Repress Criminali

Dir. 1148/2016
Data Breach

**Dir. 101/2018 sett)
e.Privacy e dir-NIS**

General
Data
Protection
Regulation



70 PROMUOVIMENTI !

Data subject
Data controller
Data processor
Personal data

Reg.2016/679



**DIR. E-Privacy
DATI
NON
PERSONALI**

Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on a framework for the free flow of non-personal data in the European Union
(SWD(2017) 304 final)
(SWD(2017) 305 final)



Position Paper
Osservazioni
alla Proposta di
Regolamento sul
libero flusso dei
dati nella Unione
europea
Settembre 2017

Block Chain Mondiale

CC Sec Initiative - EU unified ICT Platform
Dopo i dati personali anche quelli non personali !

SEFT Srl - 2018

5



Reg.2016/679

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



SalvoFerraro

37







SalvoFerraro

Reg.2016/679

Non obblighi vessatori ma opportunità e vantaggio di business
Dati sono la fonte d'energia della Economia Digitale

38



Informativa

Dati «PARTICOLARI»

BY Design

Decreto L. 196/93

Reg. 679/2016

Dlvo 318/99

ADS

Consenso

Restituzione

Misure idonee di Sicurezza

Assoluto Privacy

39

Terminologia e Glossario

General
Data
Protection
Regulation



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 ...



40



Reg.2016/679

Elementi Fondanti della Data Protection
Dalla Dir 95/46 al GDPR



SalvoFerraro

Accountability: responsabilità globale Titolare politiche sistemiche (Art. 24-26)
Trasparenza: flussi transfrontalieri (periodi di conservazione)
Sistema di gestione: Documentazione, Struttura organigramma (Art.3), deleghe/audit indipendente
Sanzioni: fino ad un milione di € o 2-3% del fatturato di una holding (anche internazionale se sede IT) (Art.82/83)
Ruoli DP: Joint controllers, nomine di soggetti responsabili interni e/o esterni
Data Protection Officer: Art. 37,38 e 39, natura indipendente, supporto TDT e consorziale
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. 20
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

41

GDPR-EU e Reg.679/2016

Elementi TUP

Stesso nome/concetto
Stesso nome/concetto
Diverso nome/concetto
Diverso nome/concetto
Assente nome
Vecchi nomi
Eccezioni opposte



Elementi GDPR

Stessa funzione /attività
Diversa funzione /attività
Stessa funzione /attività
Nuova funzione /attività
Nuova funzione /attività
Deprecati /assenti
Coordinam. Es. Art.130

Tutte le Riforme sono uguali : **cambio tutto cambio nulla**

42

Concetti e approcci rivoluzionari

Art. 25 - un nuovo paradigma non un vecchio paradosso ...

Non c'è Amministrazione Digitale 2.0 senza Privacy

... Allora esiste un Designer !

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

**Privacy by design
Privacy by default**

EUROPEAN DATA PROTECTION SUPERVISOR

Dalla protezione alla Resilienza

Per non stare in corsia di emergenza tutti i giorni ...

PEN Test
IDS/IPS
V.A.
UTMs

Ispezione parte dal Registro dei Trattamenti

9 PRINCIPI di TRATTAMENTO Art. 5.1/5.2

- Liceità
- Correttezza
- Trasparenza
- Limitazione della finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità
- Riservatezza

Reg.I.T.
ART. 30,35, 36 - C.do 89,96

Campo di DBA
limitazione record

LICITA'

INTERESSE LEGITTIMO

il CONSENSO
l'adempimento ad **OBBLIGHI CONTRATTUALI**
gli **INTERESSI VITALI** della persona interessata o di terzi
gli **OBBLIGHI DI LEGGE** cui è soggetto il Titolare
l'**INTERESSE PUBBLICO** o l'**ESERCIZIO DI PUBBLICI POTERI**
l'**INTERESSE LEGITTIMO** prevalente del Titolare o di terzi cui i dati vengono comunicati.

ART. 6 par. 1, 7 - C.do 89,96

LICITA'

AMBITI DI APPLICAZIONE INTERESSE LEGITTIMO

1. Libertà di stampa e di espressione
2. Marketing diretto
3. Comunicazione politica
4. Campagne di raccolta fondi delle organizzazioni non lucrative
5. Recupero crediti anche stragiudiziale
6. Prevenzione frodi, anticiclaggio
7. Controllo indiretto dei lavoratori
8. Segnalazioni di illeciti (whistle-blowing)
9. sicurezza fisica
10. Sicurezza informatica e delle reti
11. Ricerca storica, scientifica e statistica
12. Ricerche di mercato (comprese ricerche di marketing)

ART. 6 par. 1, 7 - C.do 89,96 - dimenticheremo Ex Art. 24 comma 1 Lettera g come Interpello Ex Art.17

ART. 15, C.do 146 coord. Capo VIII - Danno e risarcimento

Interessato
«Chiunque» al CapoVIII

NOTA: Utente e Contraente presenti nel Codice Privacy non ci sono più !

Dato personale

«Dato o Informazione» della persona fisica

ART. 4 Comma 1 - C.do 26

Def. Invariata dal Codice Privacy
Piccole modifiche nelle Tipologie di «dato personale»

Quasiassi informazione riguardante una persona fisica identificata o identificabile (= Interessato-) con particolare riferimento a un identificativo.

Possibili identificativi

- il nome,
- un numero di identificazione,
- i dati relativi all'ubicazione,
- un identificativo online
- uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica (dati biometrici), uno o più elementi caratteristici della sua identità economica, culturale o sociale

Per Comunic. Elettroniche/Marketing si applica Dir. 2002/58/UE – persone fisiche e persone giuridiche (Abbenati)

Dato personale

«Dato o Informazione» della persona fisica

ART. 44 Comma 1 - C.do 26

Def. Invariata dal Codice Privacy
La differenza è piuttosto nelle Tipologie di dato!

Dati Particolari (art.9): ex-dati sensibili, dati genetici, dati biometrici

Dati Penali, relativi a condanne penali, reati, legati a misure di sicurezza

Dati con rischi elevati per la dignità e la libertà della persona (es. profilazione, geolocalizzazione, videosorveglianza...)

Dati comuni (es. dati anagrafici, codici identificativi, etc..)

Dati anonimi : non associabili a una persona identificata o identificabile. **A tali dati non si applica il Regolamento**

Per Comunic. Elettroniche/Marketing si applica Dir. 2002/58/UE – persone fisiche e persone giuridiche (Abbenati)

Dato Pubblico???

ART. 44 Comma 1 - C.do 26

Pubblico non è Pubblicato!

Il Garante ha sempre chiarito dal 2015 che la mera disponibilità di un dato su internet non lo rende utilizzabile per un Trattamento!

Con «PUBBLICO» si intende un dato per il quale sussiste un regime giuridico di accessibilità giuridica (Visura Camerale, liste elettorali, repertori di Open Data)

TUTTO SI RISOLVE CON L'INFORMATIVA DOVE DI DICHIARA TUTTO

MA NON E' VIETATO PER CACCIATORI DI TESTE (NON TAGLIATORI DI TESTE) – Legittimo Interesse TDT

Data Protection mutuamente Referenziale TUCE

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/EU.

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

Interazione fra due codici, l'uno delle comunicazioni e l'altro della protezione dei dati personali
Per valutare idoneità, liceità e adeguatezza delle misure di protezione dei dati personali

52

Trasparenza

ART. 5, 12 - C.do 58,100

NOVITA' INFORMATIVA

L'interessato deve sapere tutto sull'uso dei propri dati... prima!

53

Accountability

Chi, come, cosa e quando rende conto

ART. 4,24,27,28,29 - C.do 74,75,76,77,79,80,81

54

Accountability

Considerato il decimo Principio di Trattamento

- NATURE
 - AMBITO DI APPLICAZIONE
 - CONTESTO E FINALITÀ DEL TRATTAMENTO
 - RISCHI (PROBABILITÀ E GRAVITÀ PER DIRITTI E LIBERTÀ DELLE PERSONE)
- TITOLARI METTE IN ATTO LE MISURE DI PROTEZIONE TECNICHE E ORGANIZZATIVE ADEGUATE
- PER GARANTIRE IL POTER DIMOSTRARE, CHE IL TRATTAMENTO È EFFETTUATO CONFORMEMENTE AL REGOLAMENTO
- RIESAMINA E AGGIORNA DETTE MISURE QUALORA NECESSARIO
- E PUÒ DECISIONARE IL TRATTAMENTO CHE ADEGUANDO LA PROVA DEL SOGGETTO DEI SUOI OBBLIGHI

ART. 4,24,27,28,29 - C.do 74,75,76,77,79,80,81

Accountability

«DIMOSTRARE»
«COMPROVARE»
«RENDICONTARE»

ART. 4,24,27,28,29 - C.do 74,75,76,77,79,80,81

Introduzione del principio di BILANCIAMENTO

A seconda dei dati, rischi commessi il TdI contiene i costi e proporziona impiego di risorse (IT, DPO)

Legitimate Interest
Data subject does not necessarily override controllers

NOVITA'

ARTT. 4 – 11 Co 47

REGISTRO DEI TRATTAMENTI – Reg679/16 - Art. 30

Keyword: **COMPROVARE**

SONO OBBLIGATE A TENERE IL REGISTRO

- SOCIETÀ CON PIÙ DI 250 DIPENDENTI
- SOCIETÀ CON MENO DI 250 DIPENDENTI

SE IL TRATTAMENTO NON È OCCASIONALE

OPPURE SE INCLINDE DATI SENSIBILI O GIUDIZIARI

NON CONFONDERE CON IL REMINISCENTE DPS!

NOVITA'

Misure di Sicurezza basate su Rischio

RILEVANZA PENALE A CARICO DEL TITOLARE DEL TRATTAMENTO

MISURE TECNICHE/ ORGANIZZATIVE ADEGUATE PER GARANTIRE UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO, TENENDO CONTO:

- DEI COSTI DI ATTUAZIONE
- DELLA NATURA DEL TRATTAMENTO
- DELL'OGGETTO DEL TRATTAMENTO
- DEL CONTESTO DEL TRATTAMENTO
- DELLE FINALITÀ DEL TRATTAMENTO
- DEL RISCHIO PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE

Misure di Sicurezza basate su Rischio

COME FARE: pareri e linee guida più utili del Regolamento sul «come fare»

LE LINEE GUIDA INTERPRETATIVE DEL GDPR

- Linee-guida sul responsabilità della protezione dei dati (RPD) WP243 del 13 dicembre 2018 (emendate il 5.4.2017)
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento «possa presentare un rischio elevato» ai sensi del Regolamento 2016/679 WP248 del 5.4.2017 (emendate il 4.10.2017)
- Linee-guida sulla applicazione e sulla definizione delle sanzioni amministrative ai sensi del Regolamento 2016/679 – WP 253 del 3 Ottobre 2017
- Linee-guida sul diritto alla portabilità dei dati personali WP242 del 13 dicembre 2016 (emendate il 5.4.2017)
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento WP244 del 13.12.2016 (emendate il 5.4.2017)
- Linee-guida sui processi decisionali individuali automatizzati e sulla profilazione ai sensi del Regolamento 2016/679 – WP 251 del 3 Ottobre 2017
- Linee-guida sulla notificazione delle violazioni di dati personali ("data breach") - WP 250 del 3 Ottobre 2017.

OPT/IN/OUT
Libero, incondizionato, informato
Consenso
INEQUIVOCABILE (deducibile da azioni attive o comportamenti concludenti dopo Informativa)
ESPLICITO per Dati Salute, Biometrici ecc.
Sempre **PROVATO**
Soluzione tecnica
Pratica perché
Non Obbligo Scritto
BY DESIGN
BY DEFAULT

ART. 7, 17, C.do 65,66

Niente Protocollo Informativo o Amministrazione Digitale 2.0 senza DP
AGID – opportunità con molte contraddizioni per Outsource privato / Housing service

NOVITA'
PA e Privato
non più duellanti

NOVITA'

Diritto all'oblio
Secure Erasure
De-Indexing
Portability

ART. 17, C.do 65,66 | Art 13,20 C.do 68,73

Ambito Applicazione «Materiale»
Tutte le attività produttive e di servizio, PA e Privato

ESIMENTI
Potere giudiziale e prev. Criminalità, scopi personali o domestici o vincoli contrattuali (normative ExtraUE)

ART. 2, 3 - C.do 14,27

Ambito Applicazione Territoriale

Titolare stabilito nella UE, indipendentemente dal luogo del trattamento
Trattamento di dati di interessati che si trovano nell'UE

- Offerta di beni e servizi
- Monitoraggio del comportamento

ART. 2, 3 A3 - C.do 14,27 – 22, 25
Def. Stabimento indipendentemente dal fatto che il trattamento sia EXTRAUE
Cittadino/Interessato
Rivoluzionario!
Rispetto alla filosofia del Diritto sul Territorio
PLAYER INTERNET MONDIALE !!!

ART. 8, C.do 38, 58

NOVITA'

Social & Minori
Dir. under thirteenth

Piano di Formazione

NESSUN TRATTAMENTO CON SOGGETTI NON ISTRUITI

- Obbligo nel settore sanitario (Art. 29 tutti soggetti autorizzati)
- Differenziale per attività e trattamento – Percorsi aula/eLearning
- Art. 32- Accesso ai dati solo dopo istruzione (frontali, scritte)
- Verbalizzazione Piano di Formazione (MSDP – crono/calendario)
- Supervisione DPO (Art. 39) AUDIT e prove finali (registrazioni)
- Obbligo da Sanzione amministrativa (Art. 83 GAT > 30% 2016)
- Comprovare accantonamento in Bilancio approvato
- Rubricata formazione nella BCR (Art. 47 – Gruppi di impresa)

Nelle PPAA – CAD, FOIA, ANAC, whistleblowing, trasparenza, controinteressati, non rifiuti

Arti. 29, 32, 39, 47 C.do 74

Autorità controllo capofila

NOVITA'

Unico interlocutore del titolare del trattamento in merito al trattamento transfrontaliero

ART. 60, 67 : Capofila Holding controlla blacklist!

One-Stop-shop Spgrtello Unico sedi/filiali UE

Profilazione on-line Automatizzata

NOVITA'

ART. 21,22,23 – C.do 70,73 – Prevenzione frodi/anticiclaggio – Progr. Fidelizzazione – DPR430/01 «concorso premi»

Basi giuridiche di frontiera Whistleblowing

NOVITA'

Consenso, Contratto, legittimo interesse, Conservazione limitata nel tempo, discriminazione, Informativa dipendenti e collaboratori, procedura dati sensibili, garanzia misure di trattamento

ART. 2 L.179 Nov 2017 – Denuncia illeciti lavoro Privato e Pubblico -

NOTIFICAZIONE NO !!!

Notificazione e Registro dei trattamenti

Cosa è la notificazione

Domande più frequenti (FAQ)

Intermediari

Link utili

Exonerati, chiarimenti e precisazioni

Compilazione della notificazione

Prima notificazione - Modifica - Cancellazione

Notificazione semplice

Consultazione del registro

Ma.....

Data.Breach Art. 34 e 24

Si intende in due Direzioni LEAKS

[illegible]



Codici di condotta e Certificazioni

ART. 40.41.42.43
 C.de 77.81.100

SARACENI



L'art. 39. Certificazione

La Commissione incoraggia, in particolare in materia di prodotti, la certificazione volontaria. **Diffusione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati** ai sensi di allegato 3, conformemente al presente regolamento, delle operazioni di trattamento effettuate dai responsabili del trattamento e dagli incaricati del trattamento, a meno conto delle esigenze specifiche dei micro, piccole e medie imprese. [...]



INFORMATICA E
SISTEMI DI
INFORMAZIONE



DATA PROTECTION
AND PRIVACY



COMPTON
TECHNOLOGY



Se adottati TQM e Certificazioni possono semplificare

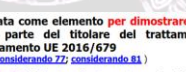
76



Codici di condotta e Certificazioni

ART. 40,41,42,43
C.de 77/81,100

Scanned with CamScanner



- Può essere utilizzata come elemento **per dimostrare il rispetto degli obblighi** da parte del titolare del trattamento e la **conformità** al Regolamento UE 2016/679
(considerando 77; considerando 81)
- **Calibrare gli obblighi** di determinate categorie di titolari del trattamento e dei responsabili del trattamento
(considerando 98)
- **Migliorare la trasparenza** e il rispetto del Regolamento e consentire agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi
(considerando 100)
- **Migliorare la reputazione aziendale e la fiducia** nei confronti degli utenti per lo sviluppo del mercato digitale

Anche le **ISO9001:2015** sono basate sulla valutazione del **RISCHIO**

78



Codici di sigilli e marchi

ART. 40,41,42,43
C.do 77,81,100

Considerando 100

"Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi"



Se adottati TQM e Certificazioni possono semplificare

79



Soggetti di riferimento

ART. 40,41,42,43
C.do 77,81,100



- UNI (Ente Italiano di Normazione)
- Accredia (Ente italiano di accreditamento)
- CEI (Comitato Elettrotecnico Italiano)
- Organismi di certificazione (ODC)
- CEN (Comité européen de normalisation)
- ISO (International Organization for Standardization)



Se adottati TQM e Certificazioni possono semplificare

80



Scenario in attesa di operatività

ART. 40,41,42,43
C.do 77,81,100

CERTIFICAZIONI
(sulla base di norme pubblicate o su schemi proprietari)



CODICI DI CONDOTTA
(sulla base della Direttiva Europea 2006/123/CE - Digi 59/2010)





Se adottati TQM e Certificazioni possono semplificare

81



Un esempio pratico: schemi

ART. 40,41,42,43
C.do 77,81,100



Se adottati schemi riconosciuti TQM e Certificazioni

82

Mappare e autorizzare < Dati Particolari e Specifici > Consultazione preventiva



Libertà espressione, rapporti di lavoro, Accesso pubblico a documenti ufficiali, Ricerca scientifica, Isp. statistici, Possibili deroghe a discrezione nazionale

Preliminar Check/Interview Art. 9,10 e 36 Dati Specifici Art.85-90

Mappare e autorizzare < Dati Particolari e Specifici > Consultazione preventiva



Preliminar Check/Interview Art. 9,10 Dati Specifici Art.85-90

Documento
Valutazione
dei Rischi e
degli Impatti

P.I.A.
D.V.R.

Processo
Permanente
Delle Politiche
Del trattamento
Art. 24

ART. 35, 36 C.do 89,96 – Per trattamenti a rischio elevato

Valutazione
Impatto sulla
Privacy

P.I.A.
D.V.R.

È UN PROCESSO
OBBLIGATORIO DI
VALUTAZIONE DEL
RISCHIO

SOLO QUANDO IL
TRATTAMENTO PRESENTA UN
RISCHIO ELEVATO PER I
DIRITTI E LE LIBERTÀ DELLE
PERSONE FISICHE

ART. 35, 36
C.do 89,96

Cosa contiene la DPIA

P.I.A.
D.V.R.

Valutazioni Metrologiche!
Soglie e PKI per S.P.C.

Matrice di valutazione

	Livello 1	Medio 2	Grave 3	Catastrofico 4
Improbabile 1	Basso	Basso	Moderato	Elevato
Poco probabile 2	Basso	Moderato	Moderato	Elevato
Probabile 3	Moderato	Moderato	Elevato	Elevato
Altamente probabile 4	Moderato	Elevato	Elevato	Elevato

ART. 35, 36
C.do 89,96

Partire dalla analisi delle minacce

P.I.A.
D.V.R.

Attacchi dall'esterno

- Acquisizione indebita di dati
- Sabotaggio \ Spionaggio
- Corruzione dei dati

Disturbi da risorse interne

- Accessi non autorizzati
- Acquisizione \ Comunicazione indebita
- Perdita \ Corruzione dati

Applicazioni Non affidabili

- Perdita di prestazioni
- Inibizione accesso ai dati
- Vulnerabilità sulla sicurezza \ Fault operativi

Fonti Informative

- Intelligence
- Intelligence economica
- Controlli di Sicurezza Complessivi
- Spionaggio industriale
- Effetto di dipendenza diretta

Comunicazione non autorizzata di informazioni sensibili

Dipendenza da partner e fornitori

MINACCE

ART. 35, 36 C.do 89,96 – ISO 29134 Guide Lines per Data Risk Assessment

Integrare analisi minacce Privacy e ICT

P.I.A.
D.V.R.

Ottemperanza ai
principi privacy
(art. 5, 9)

Protezione dei dati
Personalizzati
(art. 32 oltre agli
art. 4, 5, 30, 35, 40,
83)

ISO 29100 – 29101 (Privacy Frameworks)

ISO 29151 (Code of Practice for Personally Identified Information protection)

ISO 27001/2 (Information Security Management System)

ART. 35, 36 C.do 89,96 – DOPO V.R. SI POSSONO DEFINIRE MISURE CREDIBILI!

NON CONFONDERSI: Privacy e ICT

P.I.A.
D.V.R.

Privacy Impact Assessment

ICT Risk Assessment

Framework/Standard di riferimento:

ENISA: Privacy and Data Protection by Design

OASIS: Privacy Management Reference Model and Methodology (PMRM)

ART. 35, 36 C.do 89,96 – PIA: PRIMA (By Design/Default) PIA: in corso... e ciclico sul sistema

Chiese e associazioni religiose

Corte di giustizia dell'Unione europea
COMUNICATO STAMPA n. 10310
Lussemburgo, 10 luglio 2015

Sentenza nella causa C-201/17
Tietzsegen/Halliburton/Johansen Indesit – ukonroivnen yhtiöryhmä

Una comunità religiosa, come quella dei fedeli di Genova, è responsabile, congiuntamente ai suoi membri predicatori, del trattamento dei dati personali raccolti nell'ambito di un'attività di predicazione porta a porta.

I trattamenti di dati personali effettuati nell'ambito di un'attività di questo tipo devono rispettare le norme del diritto dell'Unione in materia di protezione dei dati personali.



NOVITA'

ART. 91, C.do 165 – Applicazione conforme diritto costituzionale nazionale e rispetto Art. 17 TFUE

I.o.T. – BYOD – CC – DOCKERS – WEB 4.0

Chi coordina tutte le attività e il piano di adeguamento ?

Evoluzione delle tecnologie ICT

necessità o adempimento formale

ART. 35, 36 C.do 89,96



D.P.O. O R.P.D

NOVITA'

1. Integra OT e IT
2. Trova strategie
3. Econometrizza
4. Test resilienza
5. Saggia selez Ext

ART. 37, 38 e 39 C.do 24, 91,97



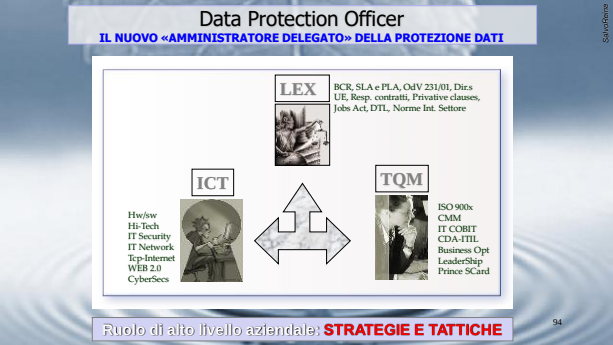
Data Protection Officer
IL NUOVO «AMMINISTRATORE DELEGATO» DELLA PROTEZIONE DATI

LEX
BCR, SLA e PLA, QdV 231/01, Dics UE, Resp. contratti, Privative clauses, Jobs Act, DTL, Norme Int. Settore

ICT
Hw/sw
Hi-Tech
IT Security
IT Network
Top-Internet
WEB 2.0
CyberSecs

TQM
ISO 9000
CMM
IT COBIT
CDA-ITIL
Business Opt
Leadership
Prince Scard

Ruolo di alto livello aziendale: STRATEGIE E TATTICHE



Riassumiamo pilastri della riforma
Chi si occupa della lista della spesa del GDPR ?

DPO/RPD consulenza indipendente per TDT e RDT che rimangono responsabili !

Accountability : responsabilità globale Titolare per politiche DP (Art. 24-26)
Trasparenza : flussi transfrontalieri interessato/terzi (periodi di conservazione) (Artt. 5,12,44 50)
Sistema di gestione : Documentazione, Strutt.Org (Art.3), deleghe/audit indipendenti
Sanzioni : fino ad un milione di € e/o 2-4% fatturato holding (internazionale sede IT-EU) (Artt.82/83)
Ruoli DP : Joint controllers, nomine di soggetti responsabili interni e/o esterni (Art. 4/28)
Data Protection Officer : Art. 37, 38, 39 indipendente, supporto TDT, obbligatorio PA, consorzio
Audit periodici : Interni e per outsource anche solo indirettamente coinvolti nei trattamenti
Diritto portabilità : migrazioni tecnologiche ICT/Cloud Computing (ITIL, CoBIT e CSA); Art. 20
Diritto all'Oblio : Rafforza facoltà controllo utenti sui propri dati Art. 17 e Art. 4 c1 Secure Erasure.
Data Retention : preservazione dato con adeguamento reale misure di **accesso al dato (limit/oblio)**



Reg.679/16 sulla Data Protection

GIA' AL PRIMO ANNO

- 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**

2009 15% incrementale nell'ultimo report 2016 sup. 6.800M€ comminati.



Reg.679/16 sulla Data Protection

Non è solo un problema di sanzioni...

Il nuovo codice è una normativa di seconda generazione

Inibitoria e Caducante

Raccoglie le esperienze maturate in 20 anni di privacy con una miriade di provvedimenti emanati

Se la ispezione è motivata da una segnalazione, in presenza di una inadempienza
blocco dei Sistemi IT



Salvo/Roma

97

Un ingaggio scorretto

Può costare
al business
più delle
sanzioni

ART 83
G.A.T.





Cosa e come
saper fare ?



1) Lo spartito **non** è uno...

2) sicuramente la musica è dal **vivo** !

Reg.679/16 - Data Protection

ACCESSO - INFORMATIVA
CONSENSO

ARTT. DAL 13 AL 23
C.do DAL 58,73 e 47

Quisque populi ?

Diritti degli interessati a meno di interesse legittimo

101



Salvo/Roma

Reg.679/16 sulla Data Protection

INFORMATIVA - CONSENSO

La **Informativa** rappresenta la rivoluzione perché declina la credibilità sostanziale del TdT

Il **Consenso** evolve accezione semantica «**Esplicito**» e rideminsiona la rilevanza ai fini della Liceità di Tratt.

Diritti degli interessati: Art. 9 – rimane Esplicito consenso dati Sensibili

ARTT. DAL 12 AL 23
C.do DAL 58,73

Salvo/Roma

Reg.679/16 sulla Data Protection Art. 13/14

INFORMATICA - CONSENSO

La Informativa diversificata e completa

- la possibilità di revocare il consenso in qualsiasi momento;
- il diritto di proporre reclamo ad un'autorità di controllo diversa da quella riferibile al Titolare;
- l'indicazione se la comunicazione di dati personali è un **obbligo legale** o è necessario per la conclusione di un contratto;
- se l'interessato ha l'obbligo di fornire i dati e le possibili conseguenze di un rifiuto;
- se l'interessato sarà oggetto di attività di **profilazione**.

Se dati all'estero TDT obbligato a riportare RDP e DPO (se presente curerà le relazioni con gli interessati)

ARTT. DAL 13 AL 23
C.do DAL 56,73

Reg.679/16 sulla Data Protection - Artt. 13/14

INFORMATIVA - CONSENSO

La **Informativa chiara e semplice**

Art. 13 – presso interessato
Art.14 – altre vie (TDT/ Rete)

1. *Concisa*

2. *Trasparente*

3. *Intelleggibile*

4. *Facilmente reperibile dall'Interessato (WEB)*

5. *Completa*

ARTT. DAL 13 e 14

C.d.o dal 30/75

Reg.679/16 sulla Data Protection

INFORMATIVA - **CONSENSO**

Inequivocabile, deducibile da azioni attive o comportamenti concludenti

- > **informato**, prestato quindi dopo aver ricevuto una chiara "informazione" sul trattamento dei dati;
- > **libero**, **svincolato** da qualsiasi obbligo e forma, anche indiretta, di coercizione che ne renda inefficace il rilascio;
- > **limitato**, sia per quanto attiene alla sua durata che per la tipologia del trattamento per il quale viene prestato il consenso;
- > **esplicito** – opt-in, ossia non è più possibile che l'azione dell'interessato, o maggior ragione la sua inattività, possa essere considerata come manifestazione del consenso;
- > nel caso di profilazione il consenso deve essere raccolto separatamente da altre forme di consenso.

Se dati perseguono più finalità raccogliere altrettanti consensi in modo distinto!

ARTT. DAL 12 AL 23
C.da DAL 58,73

Reg.679/16 sulla Data Protection

INFORMATIVA - **CONSENSO**

Avremo ICONE standardizzate dalla UE

Come accade
Oggi per la
Videosorveglianza
ed
Arece confinate
Di rischio

Se dati perseguono più finalità raccogliere altrettanti consensi in modo distinto ma non secondo tipologia di mezzo (mail,sms,fax)!

**ARTT. DAL 12 AL 23
C.da DAL 58,73**

IL TRATTAMENTO - Reg.679/16

Tipologie di Trattamento



**Automatico
e Manuale**

Mai dimenticare che tutto si applica anche al cartaceo

Definizione della Profilazione

Tipologie di Trattamento :
qualsunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati

La raccolta,
la registrazione,
l'organizzazione,
la conservazione,
l'elaborazione,
la consultazione,
la modificazione,
la selezione,
La limitazione

l'estrazione,
il raffronto,
l'utilizzo,
l'interconnessione,
il blocco,
la comunicazione,
la diffusione,
la interconnessione
la cancellazione.

Definizione ampliata e introduzione della Profilazione come trattamento per il quale diventa obbligatoria la DPIA - Data Protection Impact Assessments

Nuovo Reg.679/16

Interessante definizione

ARCHIVIO

Il GDPR definisce archivio qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

A4, co.4

109

Reg.679/16 sulla Data Protection

TRATTAMENTI: **LA PROFILAZIONE**

Automatica di:
Dati economici (salari, bilanci, proprietà acquisizioni)
Dati econometrici (rendimenti, investimenti ecc)
Dati di salute (anche indiretti – Assenze per malattia)
Geo-localizzante (anche triangolata tramite banche dati - MDM sw)
AI per selezione del lavoro (come dato econometrico se non supervisione)

ATTENZIONE:
*non clusterizzazione/raggruppamenti
ai fini di campioni/coorti marketing diretto.*

ARTT. DAL 12 AL 23
C.do DAL 56,73

110

Nuovo Reg.679/16

Forme di Profilazione

Ad esempio, essa può essere ritenuta utile da chi la effettua per analizzare o prevedere aspetti riguardanti

- il rendimento professionale,
- la situazione economica,
- la salute,
- le preferenze personali,
- gli interessi,
- l'affidabilità,
- il comportamento,
- l'ubicazione o gli spostamenti di detta persona fisica.

A4, co.4

111

LE MISURE MINIME DI SICUREZZA
POI IDONEE E SOSTENIBILI
ORA ADEGUATE e COMPROVATE

«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

112

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

Reg.679/16 sulla Data Protection

**LOGICHE, FISICHE
Ed ORGANIZZATIVE**



Misure Adeguate Idonee e congrue quando avete l'ingaggio ispettivo
La radice etimologica confutizza il fatto che non esistono soluzioni standard ed ognuno può ideare soluzioni proprie, purché concrete, funzionali ed efficaci.

113

Reg.679/16 sulla Data Protection

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 (anti-intrusione, antincendio, 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 ISO9001/27001/20000 :
Descrivere ciò che viene fatto e non ciò che "si dovrebbe fare"



114

Cosa chiedere E COSA ESIGERE dagli informatici

Esempi semplici : Misure irrinunciabili e ovvie

Data Breach (inteso anche come perdita di disponibilità del dato)

- Gestione ACL sulle risorse e sulle attività
- Gestione e Monitoraggio Log
- Misure Proattive per sicurezza perimetrale
- Redazione e affiancamento disciplinare per tutta l'azienda
- Gestione Copie/repliche di sicurezza
 - Storizzazione (repertori pseudonimizzati)
- Notifica degli incidenti «Data Breach» Art.33 (Anche Resp.Ext.)
- Gruppo proattivo SOC/CERT

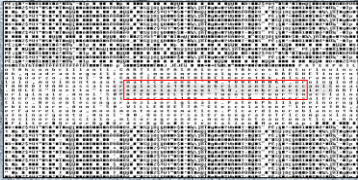


Uno occasione aziendale da sfruttare : GPO sui Servers (LDAP/AD)

115

MISURE IT CHE SONO IN REALTA' ORGANIZZATIVE

Formazione per Sistema Informativo : ES : «Spooler di stampa»



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

116

Reg.679/16 sulla Data Protection

Misure Idonee <-> adeguate di Sicurezza

DATI SENSIBILI, GIUDIZIARI o PARTICOLARI o SPECIFICI

- Norme per la custodia dei supporti rimovibili
- Procedure di Disaster recovery che prevedano il ripristino dell'accesso ai dati al massimo in 7 giorni
- Cifratura dei dati particolari/specifici e loro custodia in locali e/o contenitori di sicurezza



Dati : biometrici, genetici, sanitari di indirizzo e orientamento

117

I CRITERI DI DISASTER RECOVERY ART. 32

Dove necessario 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, alluvioni, smottamenti ecc)

Tre tipologie di misure

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

Due possibili piani di azione (non esclusivi)

- BCP (Business Continuity Plan) ISO 22301, BS25999
- DRC (Disaster Recovery Plan) ISO 27031



It takes 19 days to re-type 20Mb of lost data.

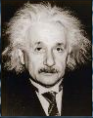
Every 15 seconds a hard drive crashes.

2000 laptops are stolen or lost every day.

ISO/SAC/BSI/CSQA: Ricordare il criterio di sostenibilità per le Piccole e Micro aziende!

118

Documentazione di Compliance



Dipende dal punto di riferimento dell'osservatore ...

QUALITA' E SICUREZZA ORIENTATE AL RISCHIO



Non è il ritorno del DPS !

120

SEFT Srl - 2018

20

Unificazione Privacy e IT Security

Compliance nell'antichità... perché non oggi?



Masterplan implementativo : NON interventi Ex Post

Unificazione Privacy e IT Security

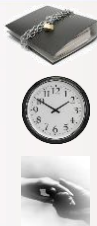
Concetti funzionali della compliance:

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)



Unificazione Privacy e IT Security

C'ERA UNA VOLTA IL DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

L'epica di un falso problema !

Il DPS diventa il MSP con REGISTRO (Art.30)

... e fino ad oggi come avete fatto ?

General Data Protection Regulation

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

Unificazione Privacy e IT Security

DPS – di fatto esiste!
a non si chiama più così !

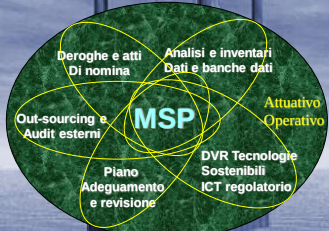
Oggi Manuale del Sistema Privacy (MSP)

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 esistono gli STATEMENTS

Reg.679/16 sulla Data Protection



NON ESISTE UN-MANUALE CARTACEO PER TUTTI

COME RENDERE CREDIBILE IL MSP

Ecco gli Statements !

Attuativo

Operativo

ATTENZIONE : Analisi dei Rischi preventiva ! Guardiamo il MindMap !!!

Reg.679/16 sulla Data Protection

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)

AgID: CAD e Prot. IT nelle PPAA

Art. 2 L.179 Nov 2017 – Denuncia illeciti lavoro Privato e Pubblico - Whistleblowing

Non solo carta...

127

REGISTRO DEI TRATTAMENTI – Reg679/16

Art. 30 – Dovuto se > 250 dip., Dati Particolari, tratt. Sistematici, larga scala

Per ciascun trattamento indicare:

Finalità e termini di cancellazione (oblio)

Modalità di trattamento (durata, tipo, UE o extra UE)

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

In pratica obbligatorio in 2 versioni: TdT e RdT

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

NOVITA' CARTACEO O ELETTRONICO

DPS

128

REGISTRO DEI TRATTAMENTI – Reg679/16 Art. 30 cascata Operativa

Pre-assessment

Analisi

Implementazione

• Ricognizione HW-SW – contrattualistica

• processi e prassi di sistema (Business, ICT)

• Consenso risorse umane e forniture

• Designazioni: soggetti, figure e team di lavoro

• Individuare investimenti, priorità e ruoli/funzioni e costi

• Progettare cronogramma del piano di adeguamento

• Formalizzare manuale e scritture transattive (Garante e fornitori)

• Redazione del Registro dei trattamenti (incluso WEB e extraLAN)

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

129

Reg.679/16 sulla Data Protection

FIGURE PROFESSIONALI E RUOLI ATTUATIVI E OPERATIVI

GDPR

Nella riforma

Soggetti che sono protetti

Soggetti che si adeguano

130

Nuovo Reg.679/16

Decreto Lg.vo 196/03

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

Soggetti autorizzati (Incaricati)

Nella riforma GDPR-UE

Data Subject

Data Controller

Data Processor

131

Data Protection : un futuro UNIFICATO di PRIVACY & IT SECURITY

Figure richieste dal Sistema di Data Protection

a) Titolare Trattamento (Controller)

b) Resp. Trattamento (Co.controller/processor)

c) Soggetti Autorizzati (Vecchi Incaricati Processors)

d) ADS (Interni/Esterni) Co-processor

(Resp., Service, arch. Sostitutiva, manut. HW ecc)

New Entry: Rappresentante (senza vignetta -->)

ART. 4,24,27,28,29 C.do 74-77, 79-81

132



Titolare del trattamento

Fulcro di tutta la riforma: CULPA IN ELIGENDO/VIGILANDO
Determina Politiche, finalità, mezzi trattamento
AD/AU cmq nomina controllo societario e vigila su RdT
Persona giuridica che può stare a giudizio per l'azienda/organizzazione

ART. 4.7 e obblighi 29

La **contitolarità** permette di condividerne l'impianto e unificare sedi in diverse locazioni / aziende consortili
Legalese: **Accordo di Riparto Interno**

Sportello unico
Dati trasparenti
Rappresentante

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

ART. 26
Parere 1/2019
Garanti UE

La **contitolarità** permette di condividerne l'impianto e unificare sedi in diverse locazioni / aziende consortili

QUANDO DUE O PIÙ TITOLARI DETERMINANO CONGIUNTAMENTE LE FINALITÀ E I MEZZI DEL TRATTAMENTO

SONO CONTITOLARI DEL TRATTAMENTO

CONTITOLARI DEVONO DEFINIRE IN MODO TRASPARENTE, MEDIANTE UN ACCORDO INTERNO, LE RISPETTIVE RESPONSABILITÀ

GESTIONE DEI DIRITTI DELL'INTERESSATO RISPETTIVE FUNZIONI DI RILASCIO DELL'INFORMATIVA

L'ACCORDO DEVE RIFLETTERE ADEGUATAMENTE

I RISPETTIVI RUOLI I RAPPORTI CON GLI INTERESSATI

IL CONTENUTO ESSENZIALE DELL'ACCORDO È MESSO A DISPOSIZIONE DELL'INTERESSATO

L'INTERESSATO PUÒ ESERCITARE I PROPRI DIRITTI NEI CONFRONTI DI E CONTRO CIASCUN TITOLARE

NON E' UNA NOVITA'

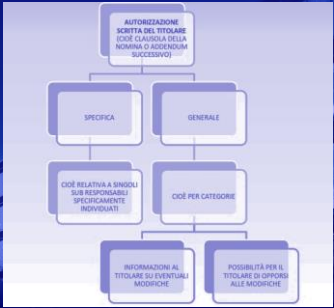
ART. 26



Responsabile del trattamento

Nomina/delega per iscritto con istruzioni operative e di ambito
Interno (HR, Resp IT, manager) / Esterno (Fornit.IT, Paghe,dematerial.)
Persona fisica/giuridica o ente che tratta i dati per conto del TdT
Integrazione contrattuale: non divulgazione se Outsource
SLA/PLA/BCR/Accordi Data Transfer

ART. 4.8 e 28 C.do 81



```
graph TD
    A[AUTORIZZAZIONE SCRITTA DEL TITOLARE  
(CUI È CAUSA DELLA NOMINA O ASSUNZIONE SUCCESSIVA)] --> B[SPECIFICA]
    A --> C[GENERALE]
    B --> D[CUI RELATIVA A SINGOLI  
SUE RESPONSABILITÀ  
SPECIFICAMENTE INDIVIDUATI]
    C --> E[CUI PER CATEGORIE]
    D --> F[INFORMAZIONI AL TITOLARE SU EVENTUALI MODIFICHE]
    E --> G[POSSIBILITÀ PER IL TITOLARE DI OPPORE ALLE MODIFICHE]
```

Responsabile del trattamento

ART. 4.8 Nomine
addizionali e
indicazioni ADS per
gruppi incaricati



Incaricati /Autorizzati al trattamento ... Designati???

ART. 4.8 – Assistenza TdT

TANQUAM NON ESSET ...
Quello che non c'è nella nomina non esiste e può essere considerata una violazione alle misure di Sicurezza (Art. 32)



L'INCARICATO
dove è finito?

Non previsto nel GDPR

Persona fisica autorizzata al trattamento
formato a mezzo ordine di servizio e
istruito con piano di formazione

ART. 28-29, C.do 80,81

Nomina Interessato
Accesso alle informazioni

Istruzioni non tutte uguali ...

Se in ufficio HR ci sono 15 incaricati, non tutti devono poter avere accesso ai dati sui permessi o referti medici. Solo quelli che trasmettono dati «sanitari» all'INAIL/INPS mentre quelli che seguono la parte amministrativa trattano dati «comuni» e sono considerati «TERZI»

Nomine «clonate» comportano rischio penale in quanto violazione di una misura di sicurezza
Semmai ricorrere a gruppi di lavoro e/o mansionario

ART. 15, C.do 146

DESTINATARIO

Introdotta nel GDPR

Persona fisica, giuridica, organismo, Autorità o servizio Pubblico che riceve i dati dell'«Interessato»

ART. 1-4, C.do 1-73

TERZO

ART. 1-4, C.do 1-73

... introdotta nel GDPR

Persona fisica che non sia Interessato, TdT, RdT, soggetto autorizzato al trattamento

142

RAPPRESENTANTE

New entry GDPR

Persona fisica o giuridica stabilita nella UE che designata dal TdT o dal RdT li rappresenta per gli obblighi relativi alla norma del Regolamento

ART. 1-4, C.do 1-73

PIANO DI FORMAZIONE a carico di RDT o Esterno

Nel GDPR –EU-2016
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 i soggetti interessati è indispensabile e mandatorio

Più cicli di formazione ad hoc per soggetto vanno 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

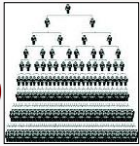
Come si fa la formazione : livelli di ruolo
(accountability, statements reintrodotte nella privacy UE)

a) Proprietà (TDT)

b) Responsabile (RDT)

c) Autorizzati (stagisti temporanei)

d) ADS (Interni/Esterni)
(Resp., Service, HW ecc)



Out-source ???

Ma tu chi sei ?

Out-source ???

adesso chiamati in correttezza secondo regime di co-controller o co-processor

Sicuramente diventano tutti Responsabili Esterni del Trattamento (Art.28)

Out-source ???

RAPPORTO TITOLARE – RESPONSABILE «ESTERNO» DEL TRATTAMENTO

CONTRATTO O ALTRO ATTO

CHE VINCOLI IL RESPONSABILE DEL TRATTAMENTO AL TITOLARE E CHE STIPULI

LA MATERIA DISCIPLINATA

LA DURATA DEL TRATTAMENTO

LA NATURA E LA FINALITÀ DEL TRATTAMENTO

IL TIPO DI DATI PERSONALI E LE CATEGORIE DI INTERESSATI

GLI OBBLIGHI E I DIRITTI DEL TITOLARE DEL TRATTAMENTO

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 contrattuali

NON DIMENTICATE IL WEB

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 scrivere accordi reciprocamente vincolanti :

- Responsabili coinvolti (nome e accettazioni iscritte)
- 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 (ISO9000:20xx)
- Private Clauses o BCR per forniture ICT

Riqualifica fornitori

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

DISCIPLINARE INTERNO per ADS / DPO

TDT dimostrare competenza ADS/DPO (contratto)

Disciplinare tecnico sul campo ... (formazione)

Protezione prese a muro e hub (misure fisiche IT)

Disattivazione device di bootstrap (BIOS - UEFI)

Protezione spool di stampa e salva schermo (comportamenti)

Tracciamento informato mailer e web incaricati (proattivo)

Dispositivi di acquisizione esterni (USB,FTP,RDP ecc.)

Criptologia estesa e piani di copie di sicurezza (liv. azienda)

Storizzazione e alter sito / locazione (Resp. e titolare Tratt.)

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 più gli imprenditori che rispondono delle Incurie tecnologiche ma devono dimostrare di non scegliere a caso



MSP è una partita di biliardo a dichiarazione...



General Data Protection Regulation

Sistema Qualità e Sicurezza basato su Governance e Compliance

Senza DPO le organizzazioni faticano e rimangono ingrate



**Accorgimenti ...
Non duplicate procedure**

Evitare : gigantismo e nanismo
Coerenza e pertinenza nelle contitolarietà !



Adattare e Adottare



READINESS !

Non saltate prima di aver cambiato prospettiva

GDPR : un nuovo paradigma

Formazione e aggiornamento

a) Evoluzione della privacy

b) **Readiness e compliance**



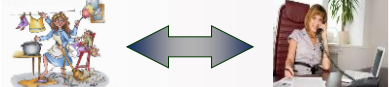
READINESS !

Privacy Enhancement Tools By ENISA

Data Protection : migrare
Da Conformità a Compliance

Dalla ispezione ... all'Audit

Dalla conformità ... alla ... Compliance!



READINESS !

Emancipare dalla logica della casalinga alla donna manager !

READINESS!

Coscienti che la vulnerabilità DP 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

Publico e Privato

EU starts building cyber-response
team

Ministero delle Infrastrutture e dei Trasporti
Dipartimento per lo Sviluppo delle Infrastrutture e dei Trasporti

15

enisa

Società del rischio tecnologico globale... Una questione che puzza di UMANO

SUCCEDERE 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 improbabile,
ciò che è improbabile ... certezza !

La Place

Considerare la privacy ICT e la CYBER-SECURITY :

- 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

READINESS!

READINESS!

Conformità <=> Compliance

Maggiori preoccupazioni di COMPLIANCE secondo EDPS

- 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 – Informativa/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 DirProvLav
- Inclusione digitale – Agenda Digitale 2.0
- Misure di backup alter loco : Sito freddo e terziarizzazioni IT
- Misure anti frode : furti di identità e preservazione contraffazioni
- Ordini professionali e accordi di settore (AGICOM, ANIA ecc..)

GDPR : New Paradigm

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)

READINESS!

Quanto costa
una breccia ?

READINESS!

Comprendere i dati raccolti e
prepararsi alla intrusione
inevitabile coordinando processi

Privacy : un nuovo paradigma
NOVITA' DEL REGOLAMENTO EUROPEO

Effetto domino : visione
danno economico !

- a) Interruzione di servizio
- b) Manutenzione straordinaria
- c) Loss of ROI
- d) Capitals Leaks
- e) Information dissemination

READINESS!

COME DECIDERE: la PNL del DPO

Formazione ripensata per la persona in azienda
Anche nelle piccole cose !
Poche basilari abitudini davanti al PC

- Gestione password su smartphone, tablet e portatile
- Creare un avviso su Google con il nostro nome
- Disconnettere sessioni dei servizi che non usiamo
- Non dare pw della propria email
- Criptare i dati sul proprio computer se USB/SD
- Abilitare la verifica in due passaggi (ES: Gmail)
- Non contanti o criptomonete in azienda
- Aggiornamenti su Facebook visibili soltanto agli amici
- Pulire la cronologia di navigazione del browser
- Mascherare il proprio indirizzo IP quando possibile

163

Dalla Sicurezza alla Resilienza...

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

Incident handling
DataBreach CIRT
First Responder
Unità di crisi

164

Come succedono le cose?

Le coincidenze non sono un cigno nero...
Deterrente **insiders** per i casi di "breccia"

It takes 19 days
to re-type 20MB
of lost data.
Every 15 seconds
a hard drive crashes.
2000 laptops
are stolen or lost
every day.

165

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

166

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

IT diventa cruciale anche ai non informatici
Esistono solo due tipi di utenti:
Quelli che hanno un PC infettato e
Quelli che **NON** sanno di avere
un PC infettato

167

Promisquità Ineluttabile irrinunciabile ?

APPLICARE **2FA** PER I BYOD

Confine sempre più sfumato tra lavoro e tempo libero
Non più **Oggetti** ma **Soggetti** che ci controllano e ci inseriscono come elementi di un eco-sistema che profila la nostra vita

168

SEFT Srl - 2018

28

Determinante anche da qui ...

Il crimine informatico

Basso rischio, opportunità e alto profitto

...

Soluzione tecnologica per le aziende...

...

Anche il business che agisce dove i Sistemi Informativi non sono curati da un ADS per la privacy

...

BLOCK-CHAIN !

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

Non-Physical ITD Cases			
Digital Communications, Storage & Integrity  eMail, Weblogs, Social Networks, File Servers, Backups, The Authentication, Integrity, Confidentiality	Authentication & Authorization  Access Control, The Security of User Sessions, Denial-of-Service	Exploitability  Malware, Botnets, Denial-of-Service, Remote Access, Denial-of-Service	Malware  Malware, Botnets, Denial-of-Service, Remote Access, Denial-of-Service
Overcoming  Detection, Abuse, Attribution, Abuse, Attribution	Defenses  Encryption	Incident Response  Investigation, Real-time, Incident Response, Incident Response	Security  Malware, Botnets, Denial-of-Service, Remote Access, Denial-of-Service
Malware & APT  Malware, Botnets, Denial-of-Service, Remote Access, Denial-of-Service	Real-time Response  Investigation, Real-time, Incident Response, Incident Response	Security & Attribution of APTs  Investigation, Real-time, Incident Response, Incident Response	

Physical ITD Cases

Currency Exchange & Remittance  Cryptocurrency, Bitcoin, Blockchain, Bitcoin, Blockchain	Anti-Fraud  Cryptocurrency, Bitcoin, Blockchain, Bitcoin, Blockchain	Anti-Money Laundering  Cryptocurrency, Bitcoin, Blockchain, Bitcoin, Blockchain	Anti-Tax Evasion  Cryptocurrency, Bitcoin, Blockchain, Bitcoin, Blockchain
--	--	---	--

READINESS!

Source: Chat Interview with the Dream Doctors, the developers of MPAack
<http://www.rbrtormos.com/2007/07/23/mpack-interview-chat-sessions/posted/>

DPO
Garante interno
Designato GRC

ARTT. 37, 38 e 39

170

Aree-Attività critiche per le quali il DPO/DPD conviene

COOSA VEDI NEL RETROVISORE

*VIRTUALIZZAZIONE CLOUD
COMPUTING - BLOCKCHAIN
DevOps, Container DOCKERS*

Dematerializzazione
Anonimizzazione dato personale
Pseudonimizzazione dato sensibili
Sec - Delocalisation BYOD / IOT
Network vs LAN-WAN - SSO

*Distributed extranet - SaaS
Corporate networks migrate CC
Persona digitale Biometry*



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 specchio retrovisore e al cui sopraggiungere non ci si può sottrarre

COME DECIDERE la compliance : **COMPETENZE del DPO**

DPO: CENTRALITA' DELLA FIGURA DP AZIENDALE

- 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)
- Principi di Risk management
(ISO 31000:2010)
- Principi di Business Continuity
(ISO 22313:2015)



172



COME DECIDERE la compliance : COMPETENZE del DPO

DPO: UN CONSIGLIERO DI FAMIGLIA



DPO: IL DESIGNER DELLA PRIVACY BY DESIGN !!!

173



*Che
tempo
farà?*

Aree critiche e Argomenti Speciali

DP in mare aperto

P4

Mini corsi sulle Aree-Attività critiche



VS e statuto lavoratori



Azienda digitale e documenti



Compliance operativa sui dati



Gestione Incidenti IT

Aree critiche e Argomenti Speciali

DP sul campo

Ano/pseudonimizzazione DB/dockers/VM

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

C.I.R.T. e I.H. per la sicurezza della sicurezza

Job's Act: Telecontrollo lavoratori

Cloud Computing e IoT

Le ispezioni del Nucleo Investigativo Privacy

BIG DATA quanto BIG?

Anonimizzazione

Minimizzazione

Pseudonimizzazione

Art. 3 e 4 – Ricorrere anche a «Segmentazione»

Anonimizzazione

Minimizzazione

Pseudonimizzazione

Dati Sanitari - eHealth

Pseudonimizzazione

I dati codificati con chiave o il ricorso a tecniche di cifratura sono un classico esempio di pseudonimizzazione. Recentemente (*Parere alla Regione Sardegna su uno schema di regolamento recante norme per il funzionamento del Registro Tumori* **25 febbraio 2016**) il Garante per la Protezione dei Dati Personali ha definito le misure e gli accorgimenti da adottare per tutelare la riservatezza degli individui cui si riferiscono i dati del Registro Tumori regionale e dei Registri Tumori locali tra i quali appunto la **pseudonimizzazione** dei dati personali degli interessati

Esempio pratico

Storia recente eredità primi provvedimenti in ambito Telemedicina, RedTech, Clinica e Diagnostica Nosocomiale

Riflessione

Chi è Sting? Gordon Matthew Thomas Sumner?



Sting

Pseudonimo e distanza del dato dall'interessato

In alcuni casi la pseudonimizzazione rende la persona più immediatamente identificabile

La pseudonimizzazione è un trattamento di dati personali

La tutela integrata nel trattamento è tutela di sicurezza

La pseudonimizzazione consiste nel sostituire un attributo solitamente univoco di un dato con un altro, ugualmente univoco e solitamente non immediatamente intelligibile

Cosa fa HASHING

Pseudonimo e distanza del dato dall'interessato

Marig Rossi = a5887a62d652d2b476e57f20bbbc8c2c

Marig Rossi = 9e8999b9d6112271d4ba56ae463ec1f

Distanza tra informazione in entrata e in uscita – dispendio economico rilevante per «reversare»

Aree critiche e Argomenti Speciali

DP sul campo

Ano/pseudonimizzazione DB/dockers/VM
CyberWAR, CyberSec, CyberSpace e DP
Data Breach – cosa è, e come si affronta
C.I.R.T. e I.H. per la sicurezza della sicurezza
Job's Act: Telecontrollo lavoratori
Cloud Computing e IoT
Le ispezioni del Nucleo Investigativo Privacy

CYBER-WAR

Un solo esercito... invisibile!

CYBER-WAR

Una guerra dove il campo di battaglia è ovunque!

CYBER-WAR

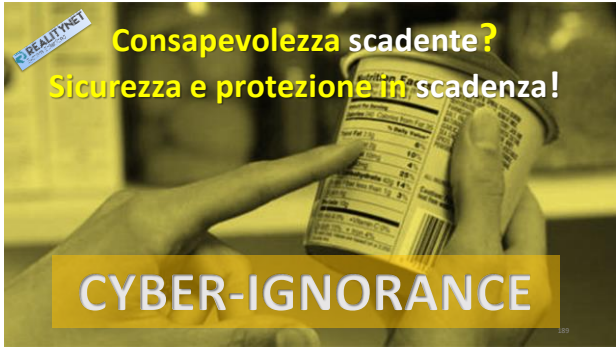
Una guerra dove non c'è il fronte!

CYBER-WAR

dove le vittime danno le loro coordinate!

CYBER-WAR

dove le vittime non sanno di esserlo !



CyberSec, CyberSpace... Cyber--- qualunque cosa

- Sicurezza Informatica e DP
- Principi della sicurezza informatica
- Minacce, vulnerabilità, attacchi ed exploit
- Maggiori minacce attuali
 - Malware
 - Password
 - Mobile
 - Cloud
- Implementazione di un piano di IT Security



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: fattori tecnologici

Un piano di sicurezza informatica è mirato a tre obiettivi fondamentali:

Riservatezza (Confidentiality)

Integrità (Integrity)

Disponibilità (Availability)



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: DISPONIBILITA'

La disponibilità è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono

Alcuni esempi di misure tecniche

- Sistemi di backup locale e remoto
- Ridondanza hardware, software e dati
- Piano di disaster recovery
- Protezione perimetrale (Firewall, IDS/IPS)
- Protezione host (Firewall, Antimalware, Data Loss Prevention)
- Gruppi di continuità
- Controllo dell'accesso fisico
- Monitoraggio delle prestazioni

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: forme di rischio

Minaccia (Threat)
Un'azione o un evento che potrebbe violare e compromettere la sicurezza di un sistema informatico

Vulnerabilità (Vulnerability)
Una debolezza o un errore di progettazione o implementazione che può portare ad un evento inaspettato o indesiderato e compromettere la sicurezza di un sistema

Target of Evaluation
Un sistema informatico, un prodotto o un componente che necessita di una valutazione sullo stato di sicurezza



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: definizioni di attacco

Attacco
ogni azione che viola o tenta di violare la sicurezza di un sistema

Exploit
Un percorso noto e definito per violare la sicurezza di un sistema informatico, sfruttando una sua vulnerabilità



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: Malware

Un **malware** consiste tipicamente in scritto codice eseguibile sviluppato con l'esplicito intento di creare danno e disservizio

In ambienti Windows, ad esempio, possiamo avere:

- File eseguibili (Executable File)
- Driver per la gestione delle periferiche (file SYS)
- Librerie condivise tra più programmi (file DLL)
- Batch script (file BAT)
- Script Perl, Python, Tcl
- VBScript, Jscript, Windows Scripting Host
- Documenti e/o altri file contenenti codice (es. DOC/DOCX, PDF, ecc.)





CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: Ransomware

“ransom” = riscatto,
“-ware” = software

Software che **criptano i dati dei computer infettati e chiedono un riscatto per lo sblocco**

Noti al mondo scientifico da oltre 10 anni, dal 2012 hanno cominciato a diffondersi e crescere in complessi e impatto

Oggi sono una delle minacce più pericolose per gli utenti privati e aziendali



Endless polymorfism

Beacons traps
Rootkits
Decoys
Breakthroughs
Hijacking
Bouncing
PW mimics
APP poisoning

Table 1: Traps according to four main types

Files	Network
- Documents (.doc, .xls, .pdf etc.) - Beacon traps - Emails - Logs - Databases - Recent/deleted documents	- Network table caches poisoning (ARP, DNS, Netbios etc.) - Mounted devices (printers, cameras etc.) - Half open connection to decoys - Host and unhost files
Applications	Credentials
- Session apps (SSH, FTP, RDP clients etc.) - Browsers (history, passwords, bookmarks etc.) - App uninstall information	- Passwords and Hash injections - Windows Credentials Manager - Password Managers

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: IL CONTAGIO e-mail

Avvio di un programma contenuto in ZIP, PDF, EXE, SCR, DOC, XLS

Programma contenuto in:

- Allegato ad email che parla di fatture, rimborsi, note di credito, spedizioni SDA, etc... anche proveniente da contatti noti
- Link alla mail
- Download da sito web di finto corriere il cui link è contenuto nell'email ricevuta (spesso su domini realistici oppure di CMS bucati)

Se non si apre l'allegato non si corrono rischi

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: IL CONTAGIO web

Navigazione su siti compromessi (Angler, CVE-2015-7645, Adobe Flash)

Pericolosi perché non richiedono intervento utente (come aprire mail)

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: **IL CONTAGIO la RETE**

Alcune versioni dei ransomware si diffondono tramite servizi RDP (porta 3389) di desktop remoto





CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: **Diffusioni pandemiche**

Nessun antivirus lo rileva nelle prime ore di diffusione



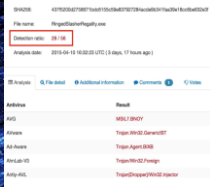


Tramite **polimorfismo** il trojan si modifica ad ogni ondata

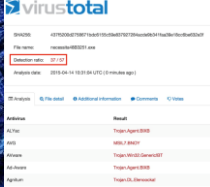
CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: **Diffusione pandemica**

A un giorno



A una settimana





CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: **IMPATTI TECNICI**

Vengono criptati documenti sulla singola macchina infetta in base a elenco:

- Doc, docx, xls,xlsx, pdf, etc...

Il sistema continua a funzionare (la vittima deve poter pagare il riscatto) a parte infezioni come Petya che "bloccano" l'intero disco (in realtà sostituiscono MBR e criptano MFT...)

Alcuni trojan criptano anche le share di rete configurate sulla macchina infetta



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: **IMPATTI ECONOMICI**

Per la singola infezione:

- ~400€ e qualche ora (nella denegata ipotesi di pagamento riscatto)
- Da qualche ora a qualche giorno (con backup)

Per contagio a più macchine via rete

- ~400€ (in alcuni casi ~400€ x n. di macchine infette) e qualche giorno (nella denegata ipotesi di pagamento riscatto)
- Diversi giorni (con backup) in particolare se criptati anche DB o applicativi



Nessuno escluso !



CyberSec, CyberSpace... Cyber---

qualunque cosa

Sicurezza informatica:

PREVENZIONE

Ma anche "semplicemente" non aprire allegati anche provenienti da contatti noti se non prima verificandoli su:

- Microsoft Word/Excel/Viewer (per file DOC/XLS)
- www.pdfonlineviewer.com o simili (per PDF)
- hybrid-analysis.com o malwr.com (ottimo sandbox e analisi di rete)
- www.virustotal.com (56 antivirus)
- urlquery.net (analisi eventuali link a siti web)



CyberSec, CyberSpace... Cyber-- qualunque cosa

Sicurezza informatica: PASSWORD LEAKAGE

Diverse grosse aziende fornitori di servizi su Internet sono state colpite negli ultimi anni

Sono state trafugate (e rese pubbliche) le credenziali di accesso di MILIONI di utenti

I database sono facilmente scaricabili!

CyberSec, CyberSpace... Cyber---

qualunque cosa

Sicurezza informatica:

PREVENZIONE

Policy aziendali sulle password

Policy aziendali sull'utilizzo/creazione di account presso fornitori terzi

Multi-factor authentication

Monitoraggio dei siti informativi

- <https://haveibeenpwned.com/>
- <https://www.leakedsource.com/>



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: IL RISCHIO E' MOBILE

Negli ultimi anni gli smartphone e i tablet sono entrati prepotentemente sul mercato e nella nostra vita quotidiana

Sono utilizzati sia a livello personale sia a livello aziendale (**corporate vs. BYOD**)

Li utilizziamo per scopi tradizionali e per svolgere attività che prima facevamo con il computer

Memorizziamo contatti, facciamo telefonate, inviamo SMS

Navighiamo su Internet, consultiamo la posta elettronica, utilizziamo diverse forme di comunicazione (Skype, WhatsApp, Viber, Facebook, LinkedIn, Twitter, ecc.)

Acquistiamo oggetti, viaggi e servizi

Accediamo al conto corrente

E soprattutto... **non ci preoccupiamo di sapere se i nostri dati sono al sicuro!**



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: IL RISCHIO E' MOBILE

OWASP TOP 10 MOBILE RISKS

M1 - Insecure Data Storage	M2 - Weak Server Side Controls	M3 - Insufficient Transport Layer Protection	M4 - Client Side Injection
M5 - Poor Authorization and Authentication	M6 - Improper Session Handling	M7 - Security Decisions via Untrusted Inputs	M8 - Side Channel Data Leakage
M9 - Broken Cryptography	M10 - Sensitive Information Disclosure		

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: CONTROLLO ACCESSI

Dati sensibili dell'utente possono essere memorizzati all'interno del dispositivo in modo **non sicuro**

- Username, passwords, cookies, authentication tokens, location data

A volte **dipende dall'applicazione e dal suo programmatore**

- Memorizzazione di credenziali in modo non cifrato all'interno di file di testo, plist, database SQLite
- Dipendenza da una master password debole
- "The mobileleak project: Forensics methodology for mobile application privacy assessment," Stirparo, P.; Kounellis, I., <http://eeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6470964&arnumber=6470811>

A volte **dipende dall'utente/azienda** che non configurano in modo adeguato il dispositivo seguendo le linee guida



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: GEOLOCALIZZAZIONE



Telecontrollo lavoratori
Promisquità BYOD

**Adattare al Jobs Act
Sanzionato con la Privacy**

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: CHATTIAMO ???



Telecontrollo lavoratori
Promisquità BYOD

**Adattare al Jobs Act
Sanzionato con la Privacy**

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: NO GO SOCIAL !!!

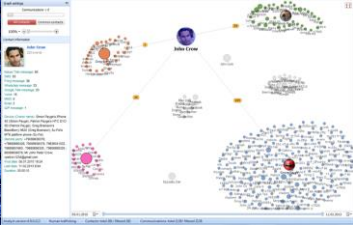


Telecontrollo lavoratori
Promisquità BYOD

**Adattare al Jobs Act
Sanzionato con la Privacy**

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: SO WE GET ALL !!!

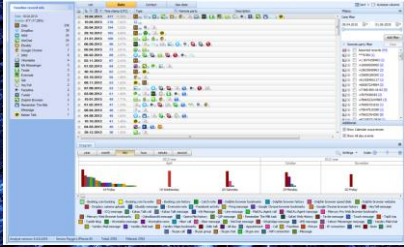


Telecontrollo lavoratori
Promisquit  BYOD

Adattare al Jobs Act
Sanzionato con la Privacy

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: EACH MOMENT OF LIFE



Telecontrollo lavoratori
Promisquit  BYOD

Adattare al Jobs Act
Sanzionato con la Privacy

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: ... OF EVERYONE !



Telecontrollo lavoratori
Promisquit  BYOD

Adattare al Jobs Act
Sanzionato con la Privacy

CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: SOCIAL AI ENGINES

Malgrado abbiate a disposizione il miglior firewall, IDS, antivirus ci sono ancora delle falle nella sicurezza.

Si basa sulle debolezze umane per violare il sistema

Un dipendente di un'azienda pu  fornire, involontariamente, preziose informazioni in una mail o rispondendo a una telefonata

Si cerca di sfruttare le debolezze della natura umana (fiducia, paura, desiderio di aiuto, ...)



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: SECURITY PLANS

Analisi dello status quo

Individuazione delle esigenze in funzione del rischio e della probabilit  (Analisi dei rischi)

Implementazioni di policy e procedure interne per la gestione dei dati

Sicurezza fisica

Difesa perimetrale

Cifratura

Sistemi di autenticazione multi fattore



CyberSec, CyberSpace... Cyber--- qualunque cosa

Sicurezza informatica: SECURITY PLANS

Sistema di autorizzazione

Gestione documentale

Mobile Device Management

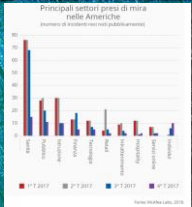
Training e awarness

Data retention

Piani e procedure di backup e disaster recovery

Pianificazione di attivit  di Vulnerability Assessment e Penetration Testing

Gestione degli incidenti e forensic readiness



Aree critiche e Argomenti Speciali

- Governance e Compliance DP
- Ano/pseudonimizzazione DB/dockers/VM
- CyberWAR, CyberSec, CyberSpace e DP
- Data Breach – cosa è, e come si affronta
- C.I.R.T. e I.H. per la sicurezza della sicurezza
- Job's Act: Telecontrollo lavoratori
- Cloud Computing e IoT
- Le ispezioni del Nucleo Investigativo Privacy

229

Data.Breach Art. 33

Torniamo al DP sul campo



230

Data.Breach Art. 33

Definizioni

Per “Violazione di dati” si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza

per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall’art. 5 del GDPR per il trattamento dei dati personali.



Dir.2009/136/EU 28 - Dlg. 69/2012 - Art. 4, comma 3, lett. g-bis Dlg.196/03 – Art. 34 Reg.679/16

231

Data.Breach Art. 33

Adempimenti

Art. 32-bis Adempimenti conseguenti ad una violazione di dati personali

Art. 32-bis1 (Adempimenti conseguenti ad una violazione di dati personali) 1) ((1. In caso di violazione di dati personali, il titolare di servizi di comunicazione elettronica accessibile al pubblico comunica senza indebiti ritardi detta violazione al Garante.

2. Quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza di persone, o di altra persona, il titolare, comunica anche agli stessi senza ritardo

utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione.

4. Ove il titolare non vi abbia già provveduto, il Garante può, considerate le presunte ripercussioni negative della violazione, obbligare lo stesso a comunicare al Garante, o ad altra persona, l'avvenuta violazione.

5. La comunicazione al Garante o ad altra persona contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni; ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione al Garante descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal titolare per porvi rimedio.

6. Il Garante può emanare, con proprio provvedimento, orientamenti e istruzioni in relazione alle circostanze in cui il titolare ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione, tenuto conto delle eventuali misure tecniche di attuazione adottate dalla Commissione europea ai sensi dell'articolo 4.



Dir.2009/136/EU 28 - Dlg. 69/2012 - Art. 4, comma 3, lett. g-bis Dlg.196/03 – Art. 34 Reg.679/16

232

Data.Breach Art. 33

Ritardo

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR, il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore



Dir.2009/136/EU 28 - Dlg. 69/2012 - Art. 4, comma 3, lett. g-bis Dlg.196/03 – Art. 34 Reg.679/16

233

Data.Breach

Procedura DP Autorità



234

Aree critiche e Argomenti Speciali

Governance e Compliance DP

Ano/pseudonimizzazione DB/dockers/VM

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

C.I.R.T. e I.H. per la sicurezza della sicurezza

Job's Act, Telecontrollo lavoratori

Cloud Computing e IoT

Le ispezioni del Nucleo Investigativo Privacy



235

Video Sorveglianza e Telecontrollo

DP dei Lavoratori ai tempi del Jobs Act

Riforma dell'Art. 4 dello Statuto dei lavoratori si ha la aggiunta del **patrimonio aziendale** che giustifica la installazione di apparati/strumenti di **Controllo a Distanza !**

GDPR non dice alcuneche rimanda Diritto Nazionale sul Lavoro Art. 88



236

Video Sorveglianza e Telecontrollo

DP dei Lavoratori ai tempi del Jobs Act

L'adozione di strumenti informatici può essere legittimo per il **Controllo a Distanza** anche a prescindere da accordi sindacali con RSU o DTL fintanto che si adottino Misure Idonee per la privacy dei lavoratori.

Garanti Europei parere n. 2/2017 dell'8 giugno 2017



237

Video Sorveglianza e Telecontrollo

DP dei Lavoratori ai tempi del Jobs Act

IMPLICAZIONI IN UN CASO CONCRETO
Ammanchi alla cassa
Installazione di telecamera occulta
Le immagini acquisite riprendono la cassiera
Furto riconducibile alla dipendente

Problemi:

- Possono essere utilizzate le immagini in sede penale (reato di furto) e in sede giurisdizionale (licenziamento)?

L'art. 4 dello Statuto dei lavoratori trova applicazione se i controlli riguardano (direttamente o indirettamente) l'attività lavorativa, mentre *devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (controlli difensivi)* quali, ad esempio, i sistemi di controllo dell'accesso ad aree riservate, o, appunto, gli apparecchi di rilevazione di telefonate "spionaggio".

(così Sent. Cass., sez. I, n. 4746/2002)

Condotte Illegittime!

Anche sentenze sul Dipendente Infedele per giustificare il Datore Lavoro.



238

SERVIZI DIGITALI CORPORATIVI: WEB, e-mail, newsletters, Cloud-SaaS

Rischio di implicazioni Civili e Penali: basta un po' di serietà!

eMails corporativa > controllo pro-attivo, responsabile automatico, forward aziendale, CC/BCC

Routers/Firewall : discriminazioni, settings filtro navigazione

Navigazione : Intranet/Extranet, VPN corporativi, Provvedimenti WEB Aziendale **OWASP - TOP10!**

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

Disciplinare LOGS : divulgato, validato in formazione, verificato periodicamente



239

Aree-Attività critiche : TdT e ADS

Archiviazione sostitutiva !

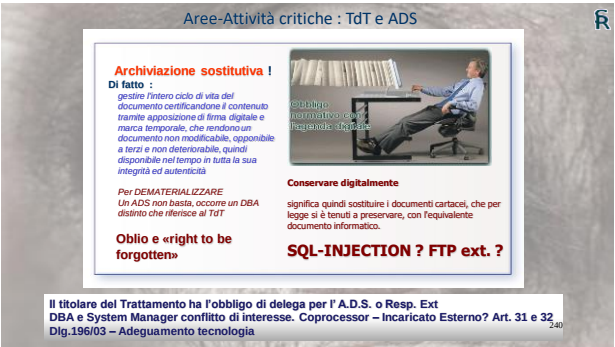
Di fatto :

- 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.

SQL-INJECTION ? FTP ext. ?

Il titolare del Trattamento ha l'obbligo di delega per l' A.D.S. o Resp. Ext DBA e System Manager conflitto di interesse. Coprocessor – Incaricato Esterno? Art. 31 e 32 Dlg.196/03 – Adeguamento tecnologia

240

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 Trossello, R&D, R&D, IndigoVision Head of Engineering

241

R

Aree-Attività critiche : TdT e ADS

Anonimizzazione
Deanonimizzazione
PSEUDONIMIZZAZIONE!

Oblio e right to be forgotten

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

?

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

... ma le Istituzioni ?

Agencia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

SPID
Sistema Pubblico
di Identità Digitale

ID

Il flop dell'identità digitale: uffici in ritardo e pochi utenti

Il salto qualitativo di marzo 2018 fissato dal governo per lo Spid. Meno della metà delle pubbliche amministrazioni si è adeguata. Passeremo unica per 2 milioni di cittadini, in gran parte per il burocrati

Il flop dell'identità digitale è la garanzia unica per i servizi della pubblica amministrazione restano nei tempi per la maggioranza degli italiani. L'obiettivo era fine marzo 2018, il target previsto nel decreto della presidenza del Consiglio del 28 ottobre 2014 su Spid Sistema pubblico di identità digitale. Entro quella data, infatti, tutte le amministrazioni pubbliche che offrono servizi on line dovevano averlo attivato per offrire un servizio anche Spid.

E negli altri Paesi come fanno ?

Iniziative Istituzionali di formazione dal 2009

UK

USA

Francia

Germania

Olanda

Molti Paesi hanno predisposto (a partire dal 2009) dei Piani di Azione di carattere Strategico per la difesa dello Spazio Cibernético.

Il nostro Garante ha fatto 8 infografiche dal 2015

SEFT Srl - 2018

41

Il nostro Garante nel 2016 per il GDPR

Più diritti per i tuoi dati !

1. **Dati take away** (portabilità dei dati)

Il tuo diritto di ricevere i tuoi dati in un formato strutturato, di comune uso e leggibile automaticamente, e di trasferirli ad un altro fornitore di servizi.

2. **Migliore trasparenza**

Il tuo diritto di sapere come i tuoi dati vengono trattati e di ricevere informazioni chiare e accessibili sul trattamento dei tuoi dati.

3. **Previdenza dei minori**

Il tuo diritto di essere protetto quando i tuoi dati vengono trattati da un fornitore di servizi che non ha i requisiti necessari per proteggere i tuoi dati.

4. **Sportello unico**

Il tuo diritto di avere un unico punto di contatto per tutte le tue richieste relative al trattamento dei tuoi dati.

5. **Servizi più elevati**

Il tuo diritto di ricevere servizi di qualità superiore grazie al tuo diritto di accesso ai tuoi dati.

6. **Diritto all'oblio**

Il tuo diritto di far cancellare i tuoi dati quando non sono più necessari o quando hai ritirato il tuo consenso.

Il nuovo Regolamento europeo sulla protezione dei dati

Dopo 4 anni di dibattito nell'UE, è stata approvata una bozza finale del Regolamento europeo sulla protezione dei dati. Un documento che dovrebbe aiutare l'Europa ad affrontare i cambiamenti dell'era digitale. Il Regolamento rafforza i diritti dei cittadini europei e offre loro un concreto strumento per il controllo dei propri dati personali. Definisce inoltre un quadro unitario di regole per le aziende e semplifica gli adempimenti previsti. Il Regolamento sarà formalmente ratificato all'inizio del 2016 ed entrerà in vigore in tutta l'Unione Europea nel 2018.

247

Aree critiche e Argomenti Speciali

Governance e Compliance DP

Ano/pseudonimizzazione DB/dockers/VM

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

C.I.R.T. e I.H. per la sicurezza della sicurezza

Job's Act: Telecontrollo lavoratori

Cloud Computing e IoT

Le ispezioni del Nucleo Investigativo Privacy

248



I vantaggi sono chiari parliamo dei problemi di contrattualità

Public, Private and Hybrid

Localisation data transfer Responsibilities identification

Impacts on consumers and actors's roles Infrastructure

Player e SLA – Provider, Broker, consumer

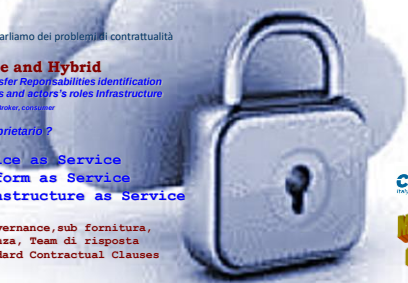
Chi è il TDT e il proprietario?

SaaS – Service as Service

PaaS – Platform as Service

IaaS – Infrastructure as Service

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



CSA IT cloud security assurance

249

A new paradigm not a new technology

What cloud is not !

Not a product nor a system... rather a MODEL

Live the paradox implying ICT players, infrastructural incumbent as well advise intermediation and final user

THE BLUE BUTTON IS TRUE **THE RED BUTTON IS FALSE**

New Mindset New Vision

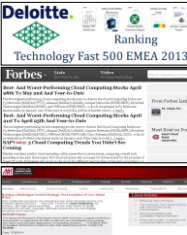




250

A new paradigm not a new technology

Who is ruling on Cloud among consulting firms?







CSA cloud security assurance **CCSK** cloud security knowledge  

251

A new paradigm not a new technology

Cloud change is everywhere, anyway! **Go Cloud or Go Home!**





CSA cloud security assurance **CCSK** cloud security knowledge  

252

SEFT Srl - 2018

42

A new paradigm not a new technology

Cloud Computing Tectonical Firms : Not just a case !

CSAcloud security intelligence

CCSKCloud Security Knowledge

ENISA

EUROPEAN COMMISSION

253

A new paradigm not a new technology

What's wrong with Cloud Controversy ?

Italy : 11% , skeptic Market, Agenda Digitale and Infrastructure Delay non the only causes.

- Too much enthusiasm
- Too much ignorance
- Too much diffidence
- Too much foreswear
- ...
- ...
- Too much of everything !!!

CSAcloud security intelligence

CCSKCloud Security Knowledge

ENISA

EUROPEAN COMMISSION

254

Why Cloud is Cloud ?

CSAcloud security intelligence

CCSKCloud Security Knowledge

ENISA

EUROPEAN COMMISSION

255

A new paradigm not a new technology

CC : Understanding conceptual implication ...

One person event ...		Consequence on multitudes
REST event ...		Volatility and virtuality
Oblivion ...		Never forgotten

CSAcloud security intelligence

CCSKCloud Security Knowledge

ENISA

EUROPEAN COMMISSION

256

Risky Challenge Era

Major implication of multi-disciplinary CC Evaluation

What is the All-in-One solution ?

Integrator on Security Advice traverses all CC elements :

Data Protection Legal advice
Trans-Border Regulatory support
Integration Investment Strategy
Cyber Protection Measures
GRC Coordination
Roadmap and SLA
Business Knowledge Migration
Business Revenue Assurance

Security

CSAcloud security intelligence

CCSKCloud Security Knowledge

ENISA

EUROPEAN COMMISSION

257

Security : critical Cloud World

Cloud & DataProtection - From SLA to PLA

On cloud the relevant legal risk is measurable I

- a) Identity (accountability)
- b) Process's Methods
- c) Location & boundary
- d) Subcontractors (tenancy)
- e) Data Tranfer Methods
- f) Security on place
- g) Monitor and Audit

CSAcloud security intelligence

CCSKCloud Security Knowledge

ENISA

EUROPEAN COMMISSION

258

[illegible]

Security : critical Cloud World

Cloud & DataProtection - From DB to HIVEs

Entity Relation Model <> OLAM & OLAPs dynaRecs



2d joined tables



3D info space















Governo Italiano
Presidenza del Consiglio dei Ministri
Consiglio dei Ministri: decreto fiscale,
decreto semplificazione, legge di
bilancio 2019

Consulto del Senato 13/10/2019 n° 23

Blockchain entra nell'ordinamento: dati e info certificati con DLT avranno valore giuridico

articolo, 18/10/2019

(Dipartimento di tecnologia basata su registri distribuiti)

1. In definitiva "tecnologie basate su registri distribuiti" le tecnologie e i protocolli informatici che sono un "registro contabile, distribuito, replicante, automaticamente bilanciamento, automaticamente decentralizzato su tutti i computer, sul cui database la registrazione la contabile, l'aggregamento e l'elaborazione di dati non si basa da ulteriormente protetti da crittografia verificabili da chiunque partecipante, non alterabili e non modificabili.
2. Altre informazioni e ai dati certificati attraverso tecnologie basate su registri distribuiti secondo il principio di immutabilità tecnologica è attribuita la stessa validità giuridica attribuita a informazioni e dati verificati attraverso l'uso di altre tecnologie.



29 / 30 settembre
STAZIONE LEOPOLDA - Firenze



Qxp IoT MAKERS

IoT
By Design
G.R.C.



Troppo di tutto

-

Troppo entusiasmo

Troppa ignoranza

Troppi attori

Troppe illusioni

Exp IoT MAKERS

263

Tropo di tutto

IOT -> IOE

-

BIG DATA

CLOUD

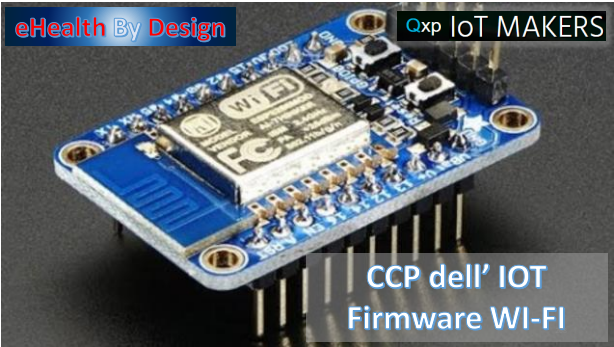
Robotics

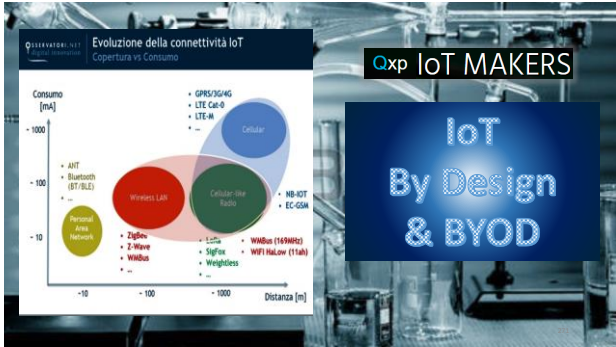
AI systems

Nano-Techs

Qxp IoT MAKERS

264





eHealth By Design **Qxp IoT MAKERS**

IoT pericolosi ?
Uso dannoso !

Big Players
Out of Date & quick obsolescence

Novel Start-Ups
No Open Source long term maintenance

eHealth By Design **Qxp IoT MAKERS**

Come si fa?

Umanizzare con la sicurezza By Design

eHealth By Design **Qxp IoT MAKERS**

IT Trans-umanista

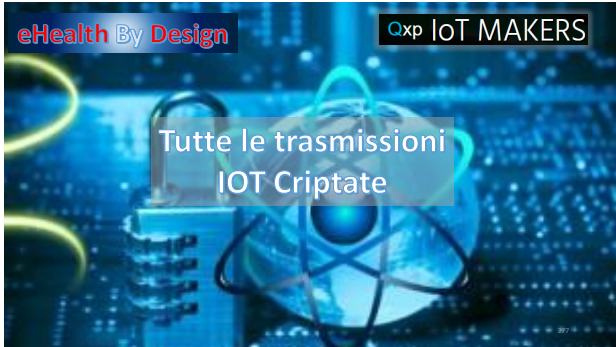
...
Temere tutto
Paura di nulla !

eHealth By Design **Qxp IoT MAKERS**

IoT By Design?
Progettazione fedele e sincera

eHealth By Design **Qxp IoT MAKERS**

... **dispositivi IoT**
tracciati in tempo reale



ISPEZIONI DATA PROTECTION E PRIVACY

Cosa è il GAT ?

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

Cooperazione nello stesso edificio: se la pattuglia in dubbio telefona Nucleo Privacy o scarica modulistica

Persecuzione di reati e crimini informatici UE-
Reg. 680/16

Esempio : *Anche durante un controllo scontrino la pattuglia che rilevasse omessa o inidonea informativa in relazione alla video sorveglianza in un esercizio può candidare per la sanzione al Garante.*

Nucleo Speciale GDF

Anti TRUST

Anti Corruzione

Privacy

Privacy : Controllo e sistema sanzionatorio

Oltre ai controlli e ispezioni sistematiche delle pattuglie fiscali

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

Tipi di controlli e ispezioni delle pattuglie

1. Dal 1999 cooperaz con Garante
2. 10/3 2016 Protoc. di Intesa
3. E-learning su territorio

La capillare disponibilità sul territorio nazionale permette un coordinamento su indicazioni della Autorità Garante così da realizzare ispezioni sistematiche secondo settori merceologici

Le pattuglie sono le stesse che controllano gli scontrini!

Privacy : Controllo e sistema sanzionatorio

Composizione della pattuglia: Ispezione preventiva

1. Due finanziari
2. Due dirig. Tecnici del Garante
3. Un ingegnere esperto Data Base

Ma le le pattuglie possono essere le stesse che controllano gli scontrini!

Privacy : Controllo e sistema sanzionatorio

controlli e ispezioni delle pattuglie come funziona?

1. Ogni anno Garante propone dei settori sulla base delle segnalazioni
2. GaT fa pre-sanzione via Rete partendo dai siti e con una e-discovery (Dark e Deep-web Nucleo Anti-Frodi tecnologiche)
3. Ispezioni riguardano quasi sempre realtà Medio-Grandi e non artigiani o negozi

Sanzioni per lo più informative, consenso, nomine e IT measures!

Privacy : Controllo e sistema sanzionatorio

controlli e ispezioni delle pattuglie

Durata della ispezione

1. Att. Ispettiva da 2 a 3 giorni
2. A meno di gravi inadempienze che possono comportare il fermo
3. Un UPG può ritenere necessario sigillatura Appareati ICT (flagranza /caducanza)

Giornalmente circa 40 militari ossia 20 pattuglie!

Privacy : Controllo e sistema sanzionatorio

controlli e ispezioni delle pattuglie
Chi controlla il controllore?

1. Reg.680/16 – Verbali pre-compilati

2. Modulo ispettivo approvato da Garante

3. Reg. 680/16 – Nuovo Modulo esteso e completo anche per PA (Ospedali, enti locali ecc)

Negli ospedali le maggiori inadempienze riguardano l'uso delle Telecamere e i Sistemi Informatici per il FSE che in Italia di fatto Non esiste!

289

Codice 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

Con il Codice Privacy da 20.000 a 175.000 euro

Introdotte aggravanti per la mancata replica :

1. Agli interessati (fax indesiderati "unsolicited practise"),

2. Alla autorità (richiesta di chiarimenti),

3. Permutazione del minimo editale (inadeguato testo difensivo)

Regolamento Europeo

quanto previsto dall'articolo 157 del Codice privacy (sanzione amministrativa)

Provvedimenti collegiali 573

276

116

26

275

580

3.179

16.193

Risposte a quesiti

54

5.282.284

I numeri del 2017

5.918

41

5.282.284

290

GDPR: Controllo e sistema sanzionatorio

Sanzioni civili, penali e amministrative...

Responsabilità penale:
solo diritto interno, ma
previa comunicazione alla
Commissione Europea

Responsabilità civile
per risarcimento del danno
Demandata al diritto nazionale
Secondo le regole di giurisdizione del GDPR

Responsabilità Amministrativa
e sanzioni amministrative: previste da GDPR
Ma comminate dall'Autorità Nazionale

Eliminazione del
ritorno

Aumento notale del
massimo

Maggior discrezionalità
dell'Autorità

Regolamento Europeo

INVERSIONE DELL'ONERE DI PROVA Art. 2050

291

Privacy : Controllo e sistema sanzionatorio

Sanzioni civili, penali e amministrative...

Sino a 10.000.000 Euro
2% fatturato se imprese (art.83 co.4)

•Violazione dei trattamenti di dati del minore anni 16/13 (art.8)

•Violazione del principio del privacy by design (art.25)

•Inadeguatezza dell'accordo di confidenzialità (art.26)

•Violazione dell'obbligo di designazione per iscritto del rappresentante nell'Unione (art.27)

•Violazioni in materia dei contenuti delle nomine e delle deleghe

•Violazione delle norme sul registro dei trattamenti

•Mancata cooperazione con Autorità (art.31)

•Inadeguatezza delle misure di sicurezza (art.32)

•Omessa notifica per data breach (art.33)

•Omessa comunicazione all'interessato (art.34)

•Violazione dell'obbligo di procedere alla valutazione d'impatto (art.35)

•Omessa consultazione preventiva o di informazioni da darsi all'Autorità (art.36)

•Omessa o inadeguata identificazione del DPO o sua inadeguata indipendenza (art.37-38)

•Violazioni del DPO

•Omessa informazioni all'Ente di Certificazione

•Violazioni degli Organismi di Certificazione

Regolamento Europeo

292

Privacy : Controllo e sistema sanzionatorio

Sanzioni civili, penali e amministrative... 2017: DATA BREACH

fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo (art.83 co.5)

• per violazione ai principi base del trattamento

• per violazione dei diritti dell'interessato (cancellazione, portabilità etc.)

• per violazioni su trasferimenti a paesi extra EU

• Violazioni ad obblighi introdotti da Stati Membro

• Inosservanza delle prescrizioni/inibizioni dell'Autorità ai sensi dell'art. 58

Giurisdizione

Stato di abituale dimora/lavoro dell'interessato

Stato ove si è verificata la violazione (residuale)

Stato ove ha sede il Titolare o il processor

Stato ove ha sede l'interessato (residuale)

ART.77

ART.79

Regolamento Europeo

293

Privacy : Controllo e sistema sanzionatorio

Sanzioni civili, penali e amministrative...

Riguarda

Controller/i (titolare/i)

Processor/i (Responsabile/i)

Ne ha diritto

Chiunque subisca un danno materiale o immateriale

Sono esonerati da responsabilità

Il titolare o il responsabile

Solo se dimostrano che alcuni non è in loro imputabile

Relazione 2017

Art. 82 Co.2 - Regolamento Europeo

294

SEFT Srl - 2018

49

Privacy : COME PREPARARSI

A proposito di controlli !!!

Da Maggio 2018 qualunque autorità della UE può effettuare controlli nelle aziende degli altri stati !

Dlg.vo 101/2018 - 19 Settembre 2018
Buona Novella o cataclisma legale?

**Privacy 4.0 – tutti sanno cosa fare...
Chi spiega come?**

Dlg.vo 101/2018: cosa contiene la Novella?

- **Abrogazione parziale Dlg.196/03 (GDPR displ.primaria)**
- **Integrazioni Dlg.196/03 – Reg.679/16 (crasi legale)**
- **Modifiche e/o rettifiche (Es. sistema sanzioni)**
- **Coordinamento normativo (Es. Statuto lavoratori)**
- **Norme transitorie Dlg.101/18 (Es. Regole di condotta)**
- **Ruolo Autorità di controllo (Prov. e prescrizioni)**

Privacy 4.0 – Adeguamento, coordinamento, integrazione

Dlg.vo 101/2018 e la Privacy 4.0

Cosa ci si aspettava...

- **Proroghe dei termini**
- **Depenalizzazioni**
- **Semplificazioni**
- **Condoni e moratorie**

Dlg.vo 101/2018 e la Privacy 4.0

E' accaduto altro !

Dlg.vo 101/2018 e la Privacy 4.0

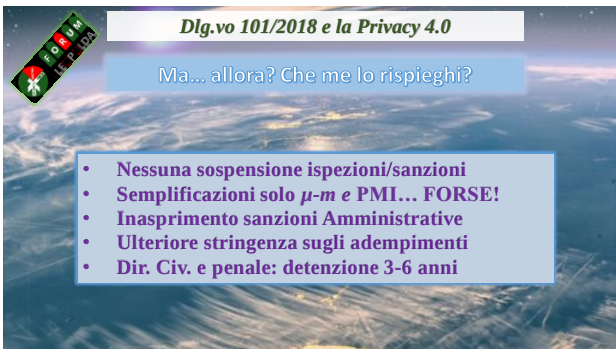
Nessuna estensione dei termini di decorrenza
Cogenza adempimenti non procrastinata!

Dlg.vo 101/2018 e la Privacy 4.0

Nessuno sconto o depenalizzazione...

Introduce «Reati Privacy»

Estrema severità del Legislatore italiano (9 reati, di cui 4 nuovi)



Dlg.vo 101/2018 e la Privacy 4.0

Ma... allora? Che me lo rispieghi?

- Nessuna sospensione ispezioni/sanzioni
- Semplificazioni solo μ -m e PMI... FORSE!
- Inasprimento sanzioni Amministrative
- Ulteriore stringenza sugli adempimenti
- Dir. Civ. e penale: detenzione 3-6 anni



FORUM
F.I.P.D.A.

Dlg.vo 101/2018 e la Privacy 4.0

SDP senza «**se**» e senza «**ma**» senza **Errori** nel SISTEMA SALUTE

- No **Cut & Paste** dei Documenti Sistemi DP
- Tutelare il dato è tutelare la **persona (paziente)**
- Non confondere **conformità** e **compliance**
- Non pensare di scaricare **oneri** a **legali** o **DPO interni**
- Formazione e consulenza: **NON FAI DA TE**

300

Dlg.vo 101/2018

Conoscere le **maggiori criticità** PRIVACY 4.0 per non inciampare



Dlg.vo 101/2018 e la Privacy 4.0

Attenzione al web !

PLA/SLA ISP
Vetrina con sigillo/marchio
Informativa completa!
Doc/Referti On-Line
Cert.OWASP Back-access
GAT e-Discovery ispezioni



Dlg.vo 101/2018 e la Privacy 4.0

Revisione globale contrattualistica affiancando tecnologo ai legali e dir. ICT
SLA, PLA, BCR, NVI - Smart Contract DAO



Dlg.vo 101/2018 e la Privacy 4.0

OPT OUT OPT IN

Informativa più importante del consenso e poi... non si chiama più informativa



Ricerca statistica, clinica, epidemiologica di pololazione sul territorio ...



Dlg.vo 101/2018 e la Privacy 4.0

Data Breach ineludibile



PERICOLO DI INCAMPO

Dlg.vo 101/2018 e la Privacy 4.0

Caducanza norma: Blocco dei dati!

Reato: Trattamento illecito reclusione fino a 18 mesi

PERICOLO DI INCAMPO

Dlg.vo 101/2018 e la Privacy 4.0

Formazione continua,
pianificata, specifica e verbalizzata

PERICOLO DI INCAMPO

Dlg.vo 101/2018 e la Privacy 4.0

Codici di Settore, di condotta, deontologici
future Regole di Condotta della AC Garante

PERICOLO DI INCAMPO

Dlg.vo 101/2018 e la Privacy 4.0

DPO vero e credibile!

RIFLESSIONI
CONCLUSIVE

In azienda : 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...





Profilo professionale

Excursus accademico e competenze

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

Expertise & skills

- Scientific Ghost-writer
- Lead Auditor – ICT Governance
- Lead Analyst – IT Security, Risk Mngmt, OHSAS
- Integrator & Advisor on 231, Dlg191/07, Dlg81/08
- Data protection officer, CDA
- Privacy & Safety Advisor & Blogger

Salvo Reina

tiro al piattello !

Certificazioni

Accreditamenti e affiliazioni

- EMAS – EMAS2
- ISO 14001:2005
- ISO 20000:2010
- ISO 27001:2009
- AM ISACA
- TÜV DPO (ISO 17024:2005)
- Ref. FEDERPRIVACY