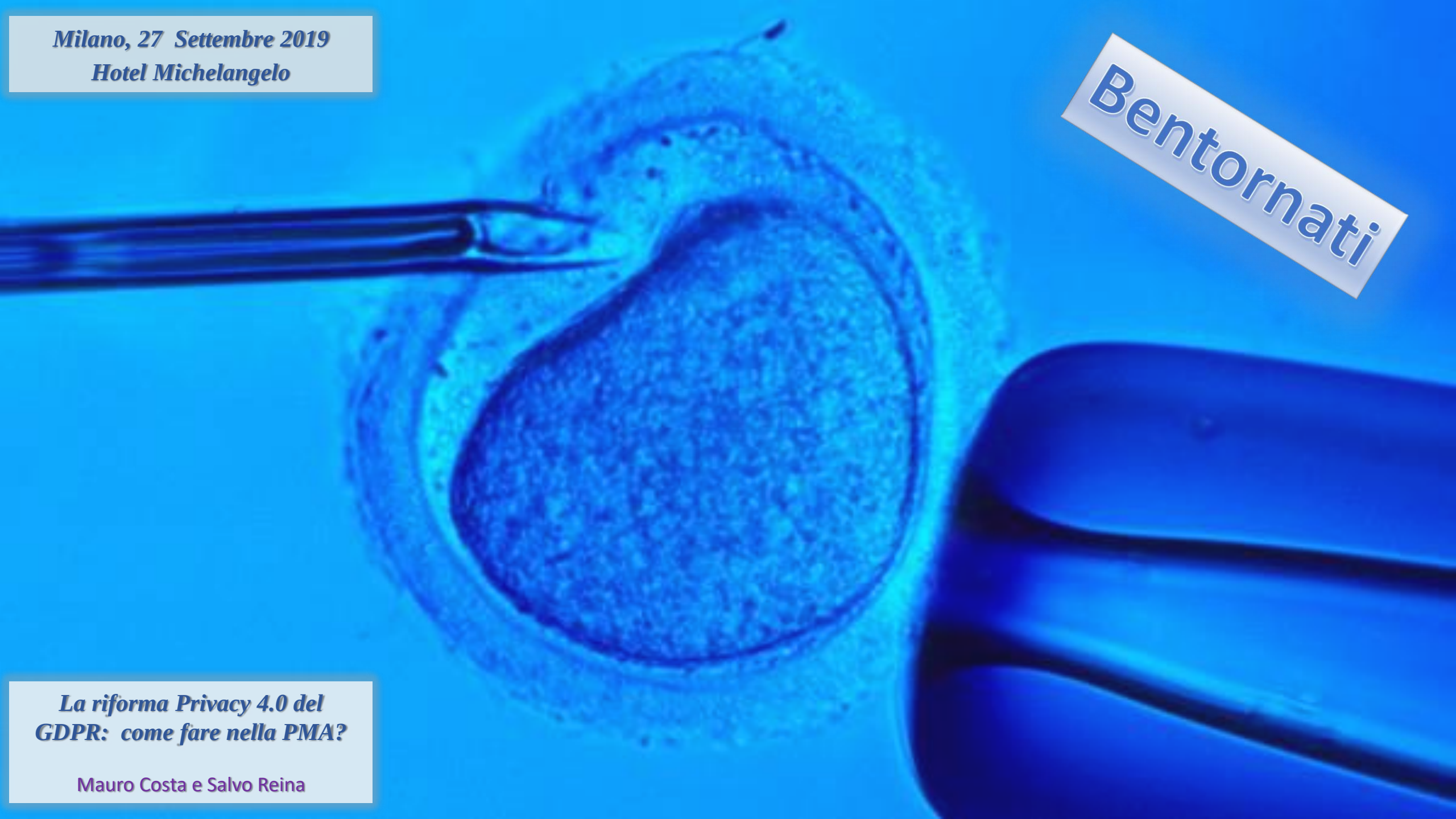
Milano, 27 Settembre 2019
Hotel Michelangelo

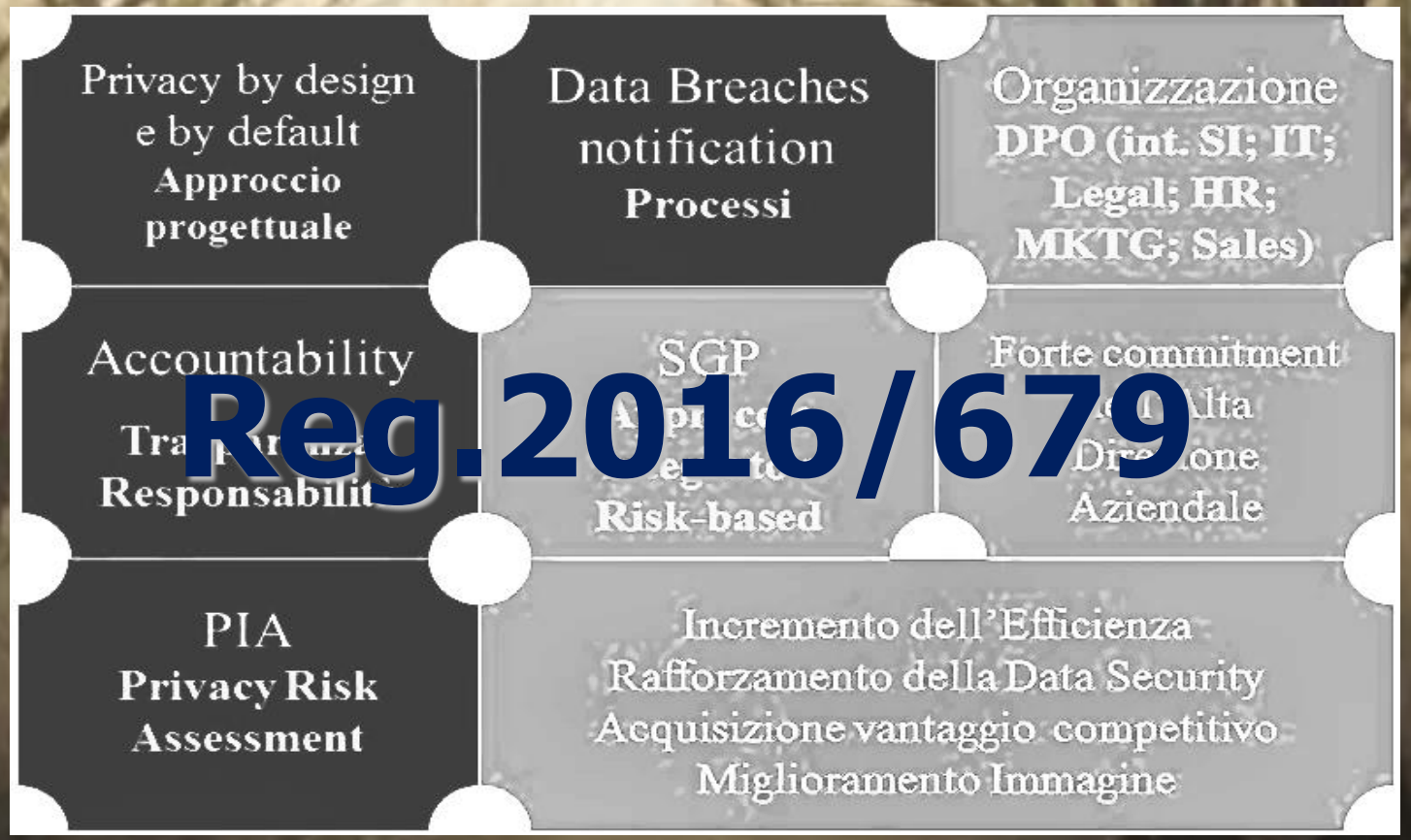


La riforma Privacy 4.0 del GDPR: come fare nella PMA?

Mauro Costa e Salvo Reina

PARTE 2

Adempimenti critici e loro implementazione nel SPPD per la PMA



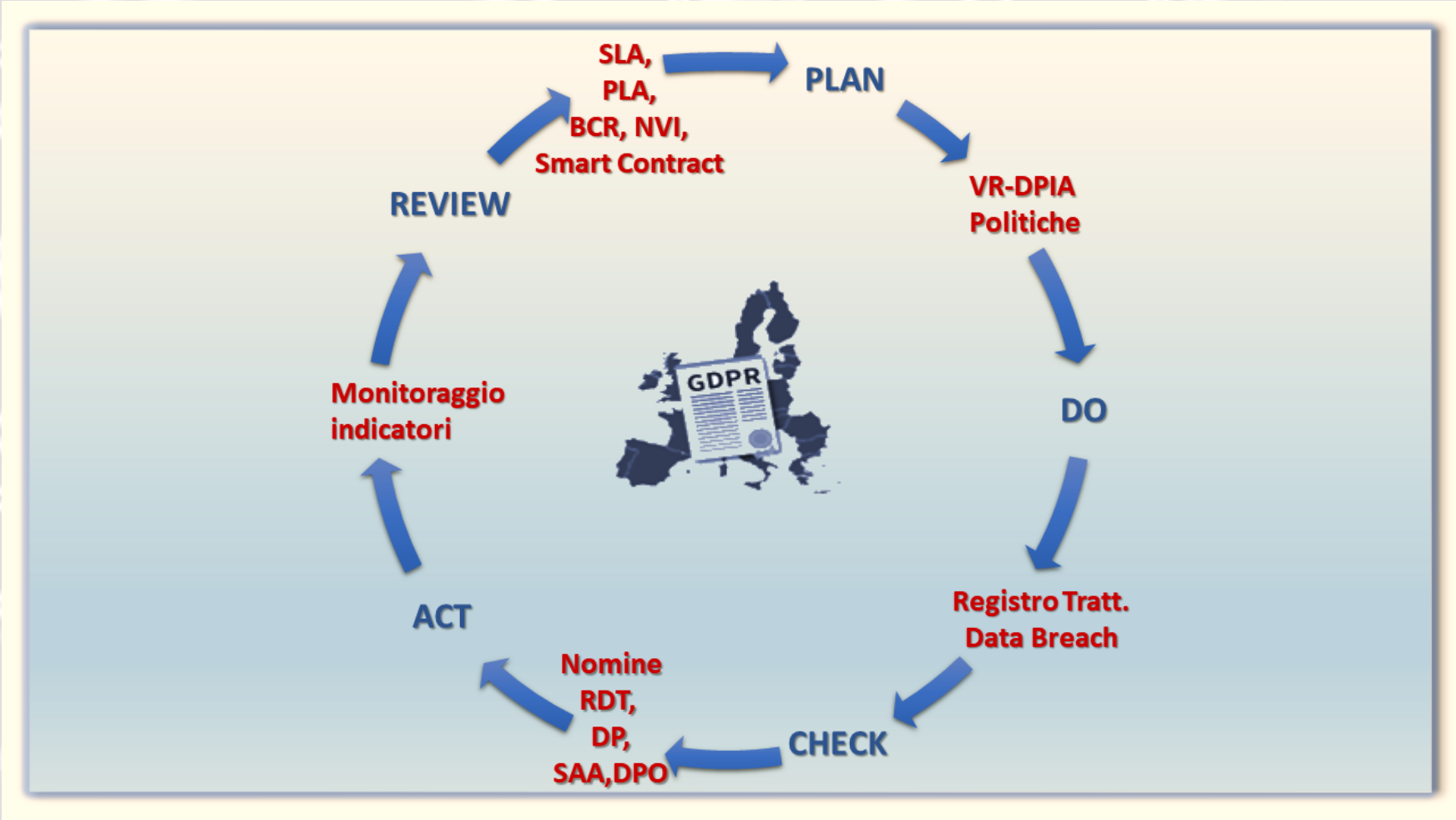
Reg.2016/679

CRITICAL CONTROL POINTS DI UN NUOVO PARADIGMA
Non obblighi vessatori ma opportunità e vantaggio di business

SalvoReina

Cosa è un SPPD

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



IMPIANTO PORTANTE: Versione giapponese del Ciclo di Deming

PARTE 2

IMPIANTO PORTANTE SPPD

- Ricognizione infrastrutture
- Censimento trattamenti
- DVR e DPIA

PRIVACY 4.0 - Da dove si parte?

SalvoReina

LA VALUTAZIONE DEI RISCHI e IMPATTI – DVR e relativo PIA

Mappare e autorizzare
< Dati Particolari e Specifici >
Consultazione preventiva

Libertà espressione, rapporti di lavoro,
Accesso pubblico a documenti ufficiali,
Ricerca scientifica, fini statistici.
Sex, Profilazioni sistematiche,
VDT biometrici, cli-diag

Preliminar
Check/Interview
Artt. 9,10 e 36
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

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

Trattamenti soggetti a DPIA

QUANDO UN TIPO DI TRATTAMENTO ALLORCHÉ PREVEDE IN PARTICOLARE L'USO DI NUOVE TECNOLOGIE, CONSIDERATI

LA NATURA	L'OGGETTO	IL CONTESTO	LE FINALITÀ DEL TRATTAMENTO

↓

PUÒ PRESENTARE UN RISCHIO ELEVATO

PER I DIRITTI	LE LIBERTÀ DELLE PERSONE FISICHE

↓

IL TITOLARE DEL TRATTAMENTO EFFETTUA, PRIMA DI PROCEDERE AL TRATTAMENTO

UNA VALUTAZIONE DELL'IMPATTO DEI TRATTAMENTI PREVISTI SULLA PROTEZIONE DEI DATI PERSONALI

ART. 35, 36
C.do 89,96

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

In PMA la DPIA è mandatoria!

VALUTAZIONE SISTEMATICA E GLOBALE DI ASPETTI PERSONALI RELATIVI A PERSONE FISICHE, BASATA SU UN TRATTAMENTO AUTOMATIZZATO, COMPRESA LA PROFILAZIONE, E SULLA QUALE SI FONDANO DECISIONI CHE HANNO EFFETTI GIURIDICI O INCIDONO IN MODO ANALOGO SIGNIFICATIVAMENTE SU DETTE PERSONE FISICHE	TRATTAMENTO, SU LARGA SCALA, DI CATEGORIE PARTICOLARI DI DATI SENSIBILI O RELATIVI A CONDANNE PENALI	SORVEGLIANZA SISTEMATICA SU LARGA SCALA DI UNA ZONA ACCESSIBILE AL PUBBLICO

ART. 35, 36
C.do 89,96

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

Chi si occupa della DPIA

IL TITOLARE	• È COLUI CHE IN ULTIMA ANALISI RIMANE DESTINATARIO DI QUESTO OBBLIGO
CON IL RESPONSABILE	• ASSISTE IL TITOLARE AL FINE DI GARANTIRE IL RISPETTO DEGLI OBBLIGHI IN MATERIA
PREVIA CONSULTAZIONE CON IL DPO	• RENDE PARERI • MONITORA L'ESECUZIONE DELLA DPIA

ART. 35, 36
C.do 89,96

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

Come si scrive una DPIA

UNA **DESCRIZIONE SISTEMATICA DEI TRATTAMENTI PREVISTI E DELLE FINALITÀ DEL TRATTAMENTO**, COMPRESO, OVE APPLICABILE, L'INTERESSE LEGITTIMO PERSEGUITO DAL TITOLARE	UNA VALUTAZIONE DELLA **NECESSITÀ E PROPORZIONALITÀ DEI TRATTAMENTI** IN RELAZIONE ALLE FINALITÀ	UNA VALUTAZIONE DEI **RISCHI PER I DIRITTI E LE LIBERTÀ** DEGLI INTERESSATI	LE MISURE PREVISTE PER AFFRONTARE I RISCHI, INCLUDENDO **LE GARANZIE, LE MISURE DI SICUREZZA E I MECCANISMI PER GARANTIRE LA PROTEZIONE DEI DATI PERSONALI** E DIMOSTRARE LA CONFORMITÀ AL REGOLAMENTO, TENUTO CONTO DEI DIRITTI E DEGLI INTERESSI LEGITTIMI DEGLI INTERESSATI E DELLE ALTRE PERSONE IN QUESTIONE

ART. 35, 36
C.do 89,96

Associare Analisi delle minacce

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

Attacchi dall'esterno	• Acquisizione indebita di dati • Sabotaggio \ Spionaggio • Corruzione dei dati
Danni da risorse umane	• Accessi non autorizzati • Acquisizione \ Comunicazione indebita • Perdita \ Corruzione dati
Applicazioni Non affidabili	• Perdita di prestazioni • Inibizione accesso ai dati • Vulnerabilità sulla sicurezza \ Fault operativi

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

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

Lo scopo della DPIA

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

Matrice di valutazione

	Lieve 1	Medio 2	Grave 3	Gravissimo 4
Improbabile 1	Basso 1	Basso 2	Moderato 3	Moderato 4
Poco probabile 2	Basso 2	Moderato 4	Moderato 6	Elevato 8
Probabile 3	Moderato 3	Moderato 6	Elevato 9	Elevato 12
Altamente probabile 4	Moderato 4	Elevato 8	Elevato 12	Elevato 16

ART. 35, 36
C.do 89,96

PARTE 2

Figure Professionali e ruoli Operativi (INTERNI/ESTERNI)

- Titolare e Cotitolari
- Responsabili e Delegati
- ADS, Soggetti Autorizzati
- …. e tutti i nuovi attori …

FIGURE PROFESSIONALI E RUOLI ATTUATIVI E OPERATIVI

Nella riforma

Soggetti che sono protetti

Soggetti che si adeguano

Nuovo Reg.679/16

e succ. Decreto Lg.vo 101/18

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

- **Il Titolare del trattamento**
- **La nomina di Responsabili (Designati, Delegati)**
- **La nomina / delega dell' ADS**
- **Soggetti autorizzati (*non Incaricati*)**
- **Terzi, Destinatari, Resp. Esterni, Delegati**

Per GDPR-UE tutti riconducibili e 3 figure

Data Subject - Data Controller - Data Processor

SalvoReina

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 /DPI

Persona giuridica che può stare a giudizio per l'azienda/organizzazione

ART. 4.7 e obblighi 29

Titolare del trattamento

ART. 4.7 - OBBLIGHI

IL TITOLARE DEL TRATTAMENTO, TENENDO CONTO DI PRECISI PARAMETRI

STATO DELL'ARTE | COSTI DI ATTUAZIONE | NATURA, AMBITO DI APPLICAZIONE, CONTESTO E FINALITÀ DEL TRATTAMENTO | RISCHI (PROBABILITÀ E GRAVITÀ)

METTE IN ATTO MISURE TECNICHE E ORGANIZZATIVE ADEGUATE

QUALI LA PSEUDONIMIZZAZIONE

VOLTE AD ATTUARE IN MODO EFFICACE I PRINCIPI DI PROTEZIONE DEI DATI

QUALI LA MINIMIZZAZIONE

E A INTEGRARE NEL TRATTAMENTO LE NECESSARIE GARANZIE

AL FINE DI SODDISFARE I REQUISITI DEL REGOLAMENTO E TUTELARE I DIRITTI DEGLI INTERESSATI

SalvoReina

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

Legalese: **Accordo di Riparto Interno**

Sportello unico
Dati transfrontalieri
Rappresentante

Condivisione di: MSPPD, ADS, INFORMATIVA, CONSENSO, DISCIPLINARE TECNICO, CREDENZIALI INFORMATICHE

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

I 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'

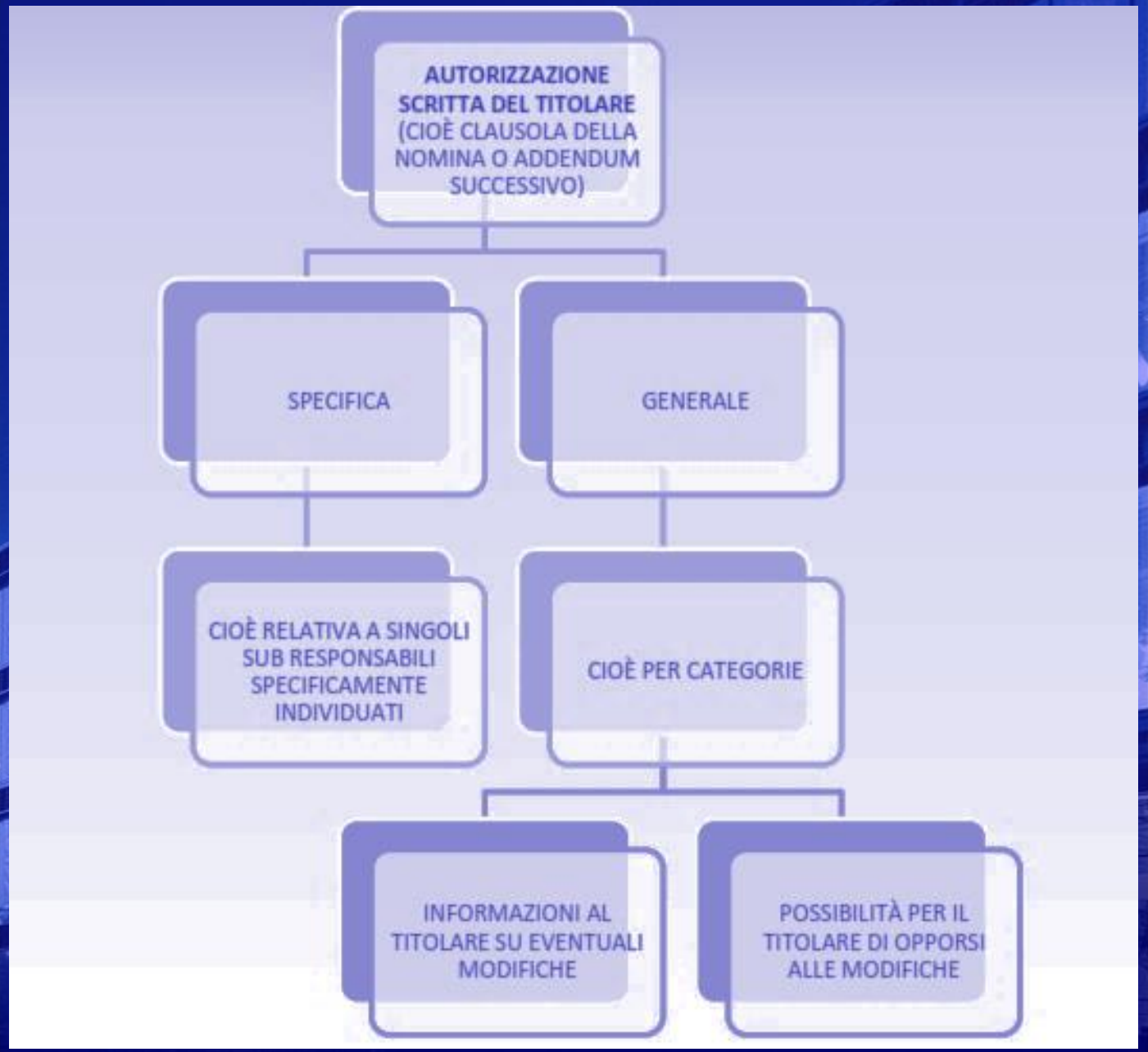
ART. 26

Il Responsabile al Trattamento oggi Delegato o Designato

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

ARTT. 4.8 e 28 C.do 81

Responsabile Delegato



ART. 4.8 Nomine addizionali e ADS e gruppi Autorizzati o Sub-Responsabili

Responsabile Delegato

IL RESPONSABILE DEVE TRATTARE I DATI PERSONALI SOLTANTO SU ISTRUZIONE DOCUMENTATA DEL TITOLARE. QUINDI:

ISTRUZIONI OPERATIVE, EVENTUALMENTE ALLEGATE ALL'ATTO DI NOMINA

VERBALIZZAZIONE DI INDICAZIONI DATE DAL TITOLARE DURANTE IL SERVIZIO, SE HANNO IMPATTO SUI TRATTAMENTI

DOCUMENTAZIONE DI INDICAZIONI MIGLIORATIVE PREVISTE A SEGUITO DI ATTIVITÀ ISPETTIVE

ART. 4.8 – coordina formazione con HR

Responsabile Delegato

- SE POSSIBILE, PSEUDONIMIZZAZIONE E CIFRATURA DEI DATI PERSONALI
- CAPACITÀ DI ASSICURARE LA RISERVATEZZA, L'INTEGRITÀ, LA DISPONIBILITÀ E LA RESILIENZA DEI SISTEMI E DEI SERVIZI
- PROCEDURA PER TESTARE, VERIFICARE E VALUTARE L'EFFICACIA DELLE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEL TRATTAMENTO

ART. 4.8 – ONERI OPERAZIONALI E VERIFICA PROCESSI

Responsabile Delegato

ART. 4.8 – Assistenza TdT

DATA BREACH

- INFORMAZIONE TEMPESTIVA
- VERIFICA DELLE CONSEGUENZE
- AZIONI DI CONTRASTO E RISOLUZIONE
- DESCRIZIONE DELL'INCIDENTE

SICUREZZA

- ALLINEAMENTO ALLE MISURE DEFINITE DAL TITOLARE IN CORSO DI RAPPORTO
- DISPONIBILITÀ A AUDIT DI SICUREZZA

VALUTAZIONE D'IMPATTO

- DISPONIBILITÀ A FORNIRE INFORMAZIONI
- COOPERAZIONE NELLE ATTIVITÀ DI VERIFICA E STESURA

L'INCARICATO
dove è finito?

Non previsto nel GDPR

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

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

Incaricati / Autorizzati
al trattamento

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)

DESTINATARIO

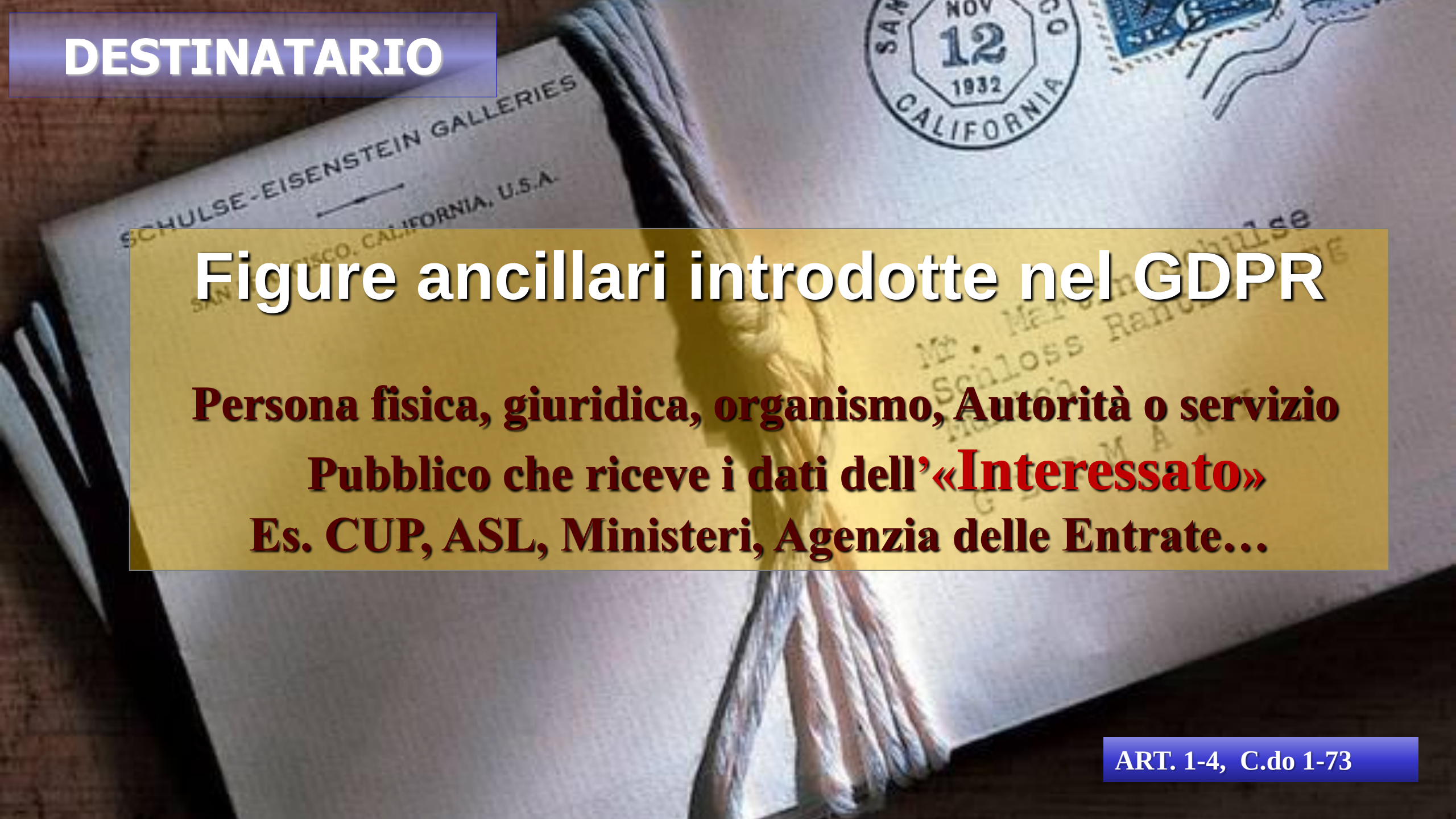


Figure ancillari introdotte nel GDPR

Persona fisica, giuridica, organismo, Autorità o servizio

Pubblico che riceve i dati dell'«Interessato»

Es. CUP, ASL, Ministeri, Agenzia delle Entrate…

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

TERZO

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

… introdotto nel GDPR

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

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


Out-source ???
Ma
tu
chi
sei
?

Out-source???

adesso chiamati in correicità 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
SLA/PLA per FORNITURE SW/HW, DAO e SERVICES ICT !

DOCS 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

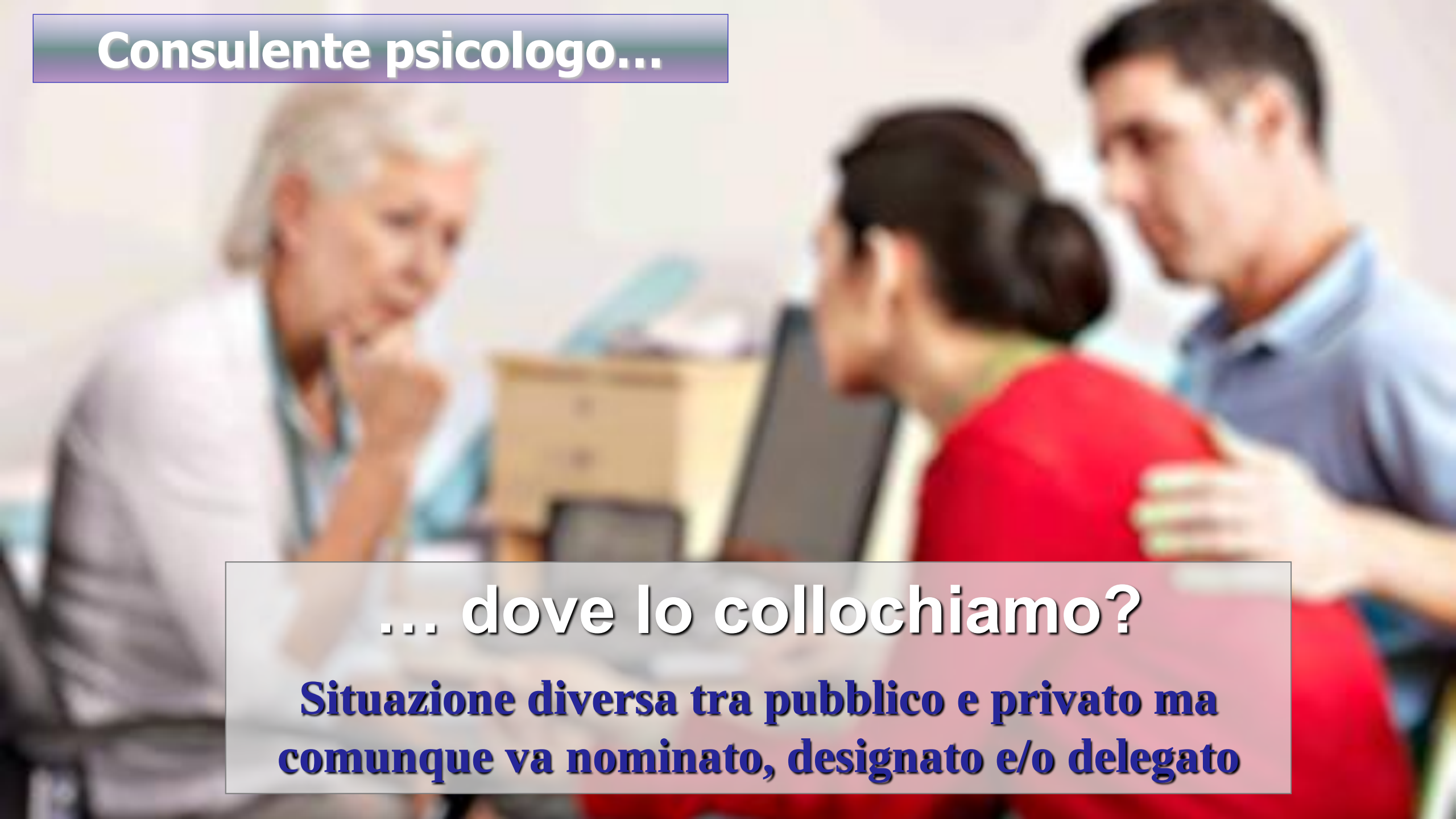
Occorre scrivere accordi reciprocamente vincolanti :

- ***Responsabili coinvolti (nomine e accettazioni iscritto)***
- ***Limiti di responsabilità assunti dal fornitore (attestato)***
- ***Misure di sicurezza del fornitore***
- ***Allegati a contrattualistica livello di servizio (SLA e PLA)***
- ***Modalità per la verifica dell'operato del fornitore (ISO90xx:20xx)***
- ***Privative Clauses o BCR per forniture ICT***

Riqualifica fornitori

In caso di incidente e/o violazione informatica chi se ne occupa e chi paga?

Consulente psicologo…



… dove lo collochiamo?

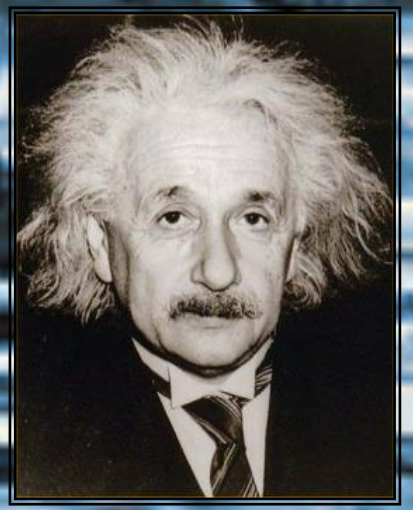
Situazione diversa tra pubblico e privato ma comunque va nominato, designato e/o delegato

PARTE 2

ISTRUTTORIA DEL MANUALE SPPD

- Nomine, deleghe / incarichi
- Nuove figure e attribuzioni
- SLA/PLA soggetti esterni

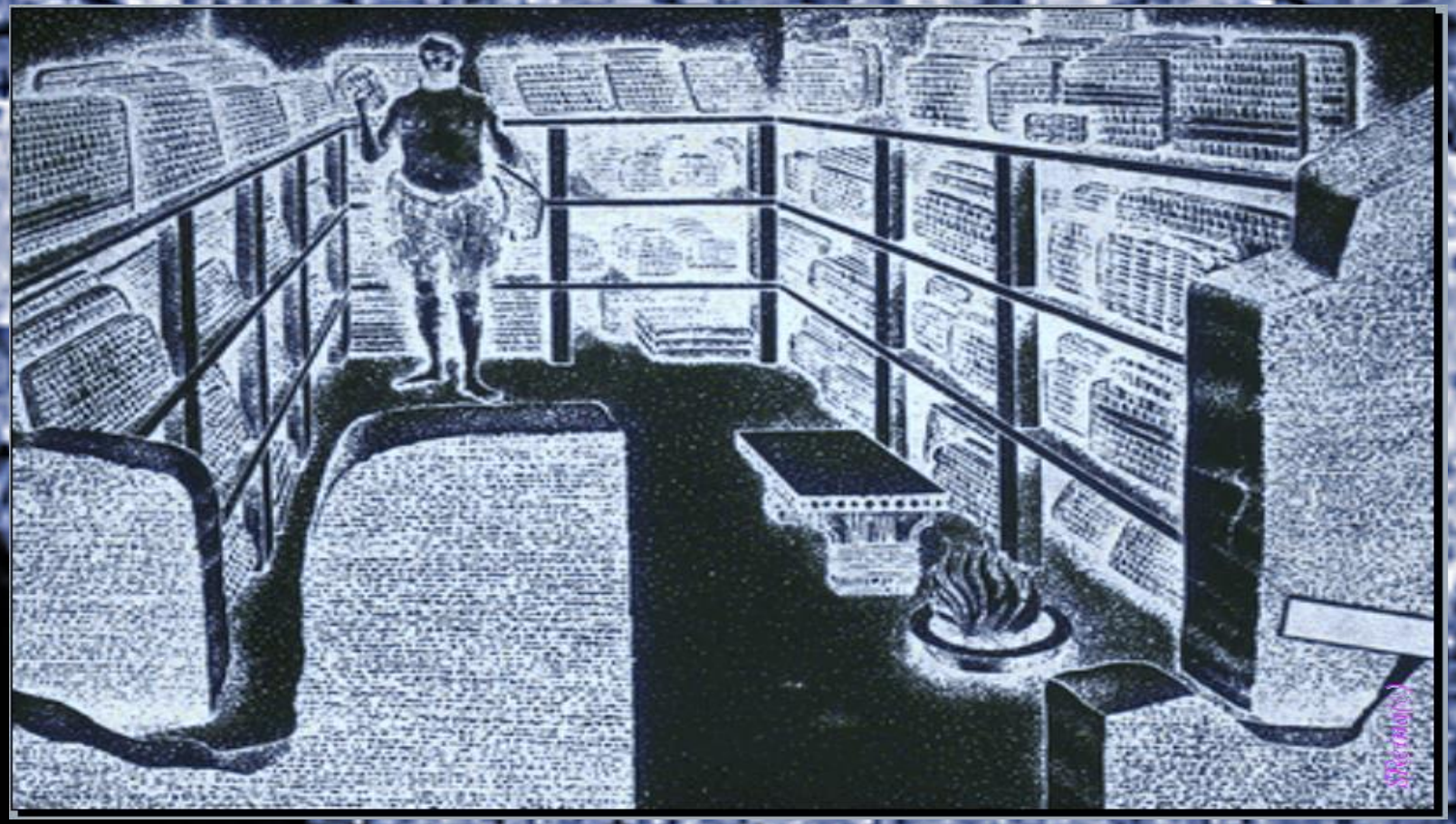
Documentazione di Compliance



Dipende dal punto di riferimento dell' osservatore …

Unificazione Privacy e IT Security

Compliance nell'antichità… perché non oggi?



Masterplan implementativo : NON interventi Ex Post

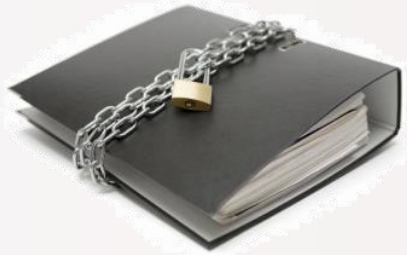
QUALITA' E SICUREZZA ORIENTATE AL RISCHIO

Non è il ritorno del DPS !

Nella Privacy 4.0 il manuale scrive

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)

È sempre un lavoro di gruppo

Coinvolgere tutto il team!

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

… per tutti i livelli della organizzazione

General Data Protection Regulation

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

Evoluzione della Privacy 4.0

DPS – concettualmente esiste ancora!
…ma non si chiama più cosi !

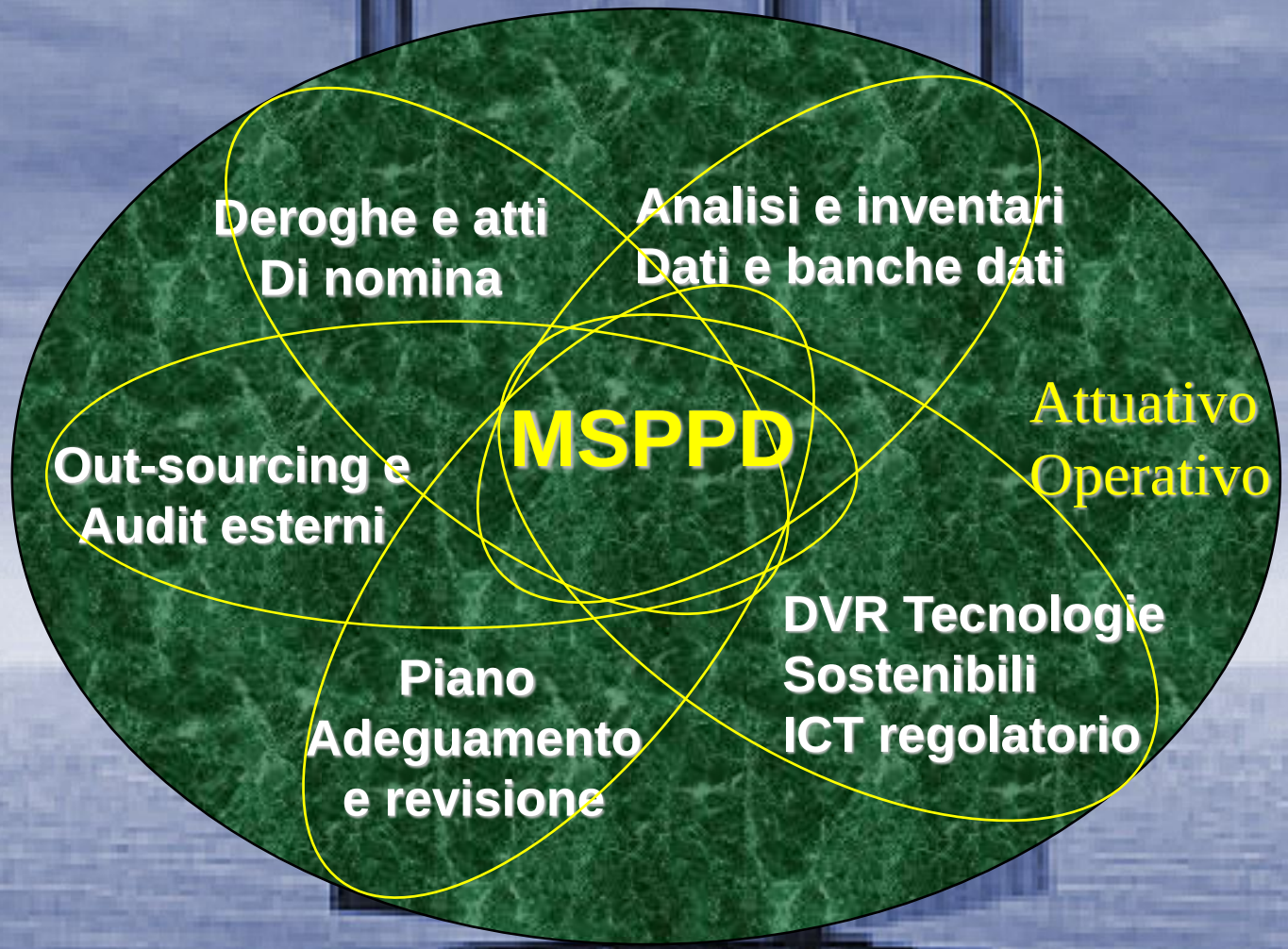
Oggi Manuale del Sistema Privacy (MSP)

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

DPS o MSP che sia rappresenta un vantaggio semplificativo di gestione

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

Reg.679/16 sulla Data Protection



NON ESISTOMO DUE MANUALI UGUALI, NEPPURE LO STESSO!

COME RENDERE CREDIBILE IL MSP

Ecco gli Statements !

Attuativo

Dichiarazioni transattive
Atti Deleghe / Nomine
Valutazione dei rischi
Inventari e Registro Trat
Scadenziari (Es Formazione)

Operativo

PIA – privacy Impact Analysis
Piano di adeguamento (PA196)
- *Procedure e prassi*
- *Istruzioni operative*

Manuale Sistema Informativo (MSI196)
Disciplinare Interno – staff

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

SalvoReina

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**

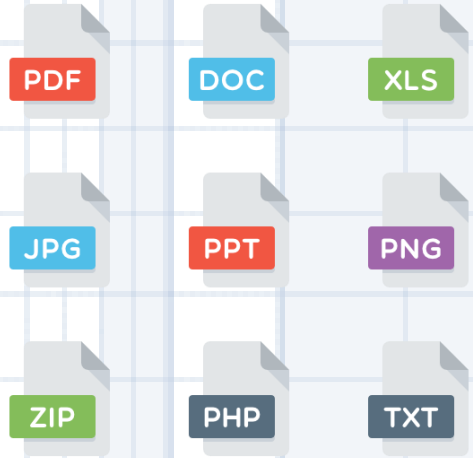
Non solo carta…

DUE REGISTRI DEL SPPD – Reg679/16 Art. 30

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***

NOVITA'
CARTACEO
O
ELETTRONICO



In pratica obbligatorio in 2 versioni: TdT e RdT

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

MSPPD – AUTOMAZIONE SOFTWARE PER TUTTO!

Attenzione a ERP/CRM/DAO e Smart Contract)

Pre-assesment

- *Ricognizione HW-SW – contrattualistica*
- *processi e prassi di sistema (Business, ICT)*
- *Censimento risorse umane e forniture*

Analisi

- *Designazioni: soggetti, figure e team di lavoro*
- *Individare investimenti, priorità e ruoli/funzioni e costi*
- *Progettare cronogramma del piano di adeguamento*

implementazione

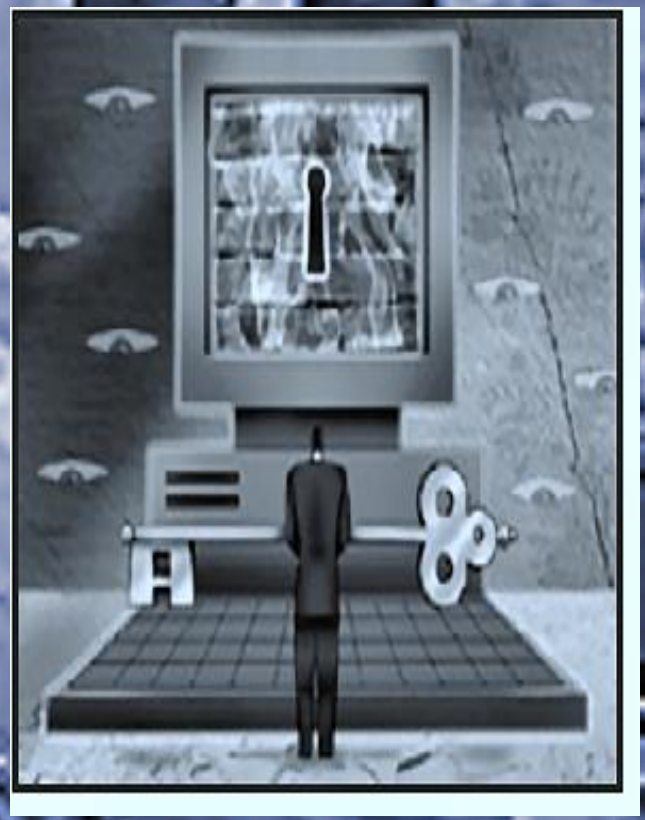
- *Formalizzare manuale e scritture transattive (Garante e fornitori)*
- *Redazione del Registro dei trattamenti (incluso WEB e extraLAN)*

NOVITA'
CARTACEO
O
ELETTRONICO

Manuale SPPD è credibile se coerente con l'Analisi dei Rischi!

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**)
Storicizzazione 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

Informativa Interessato
NEL MANUALE DEL PRIVACY 4.0

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

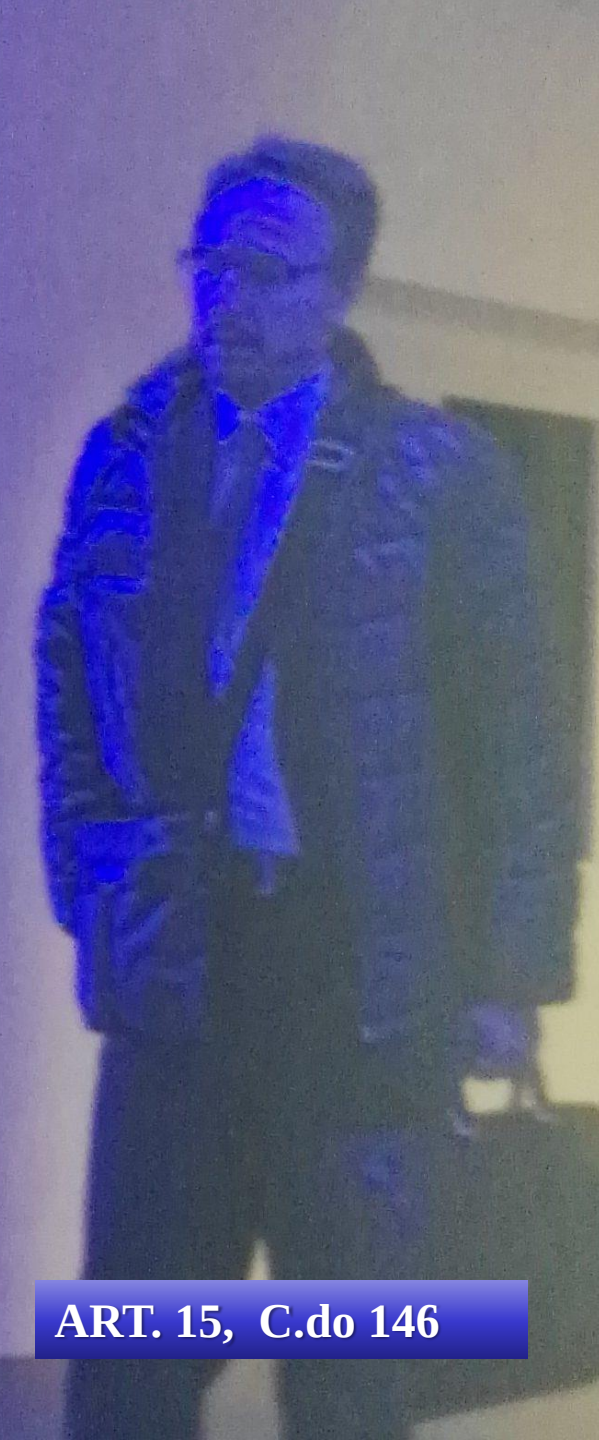
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo ad un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.



ART. 15, C.do 146

Nomine Designati
NEL MANUALE DEL PRIVACY 4.0

Istruzioni non tutte uguali …

Se in ufficio HR ci sono 15 Autorizzati, 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

MANUALE CONTIENE IL PIANO DI FORMAZIONE
Verbalizzato, documentato

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

Perché la formazione per livelli di ruolo?

(accountability, statements reintrodotti nella privacy UE)

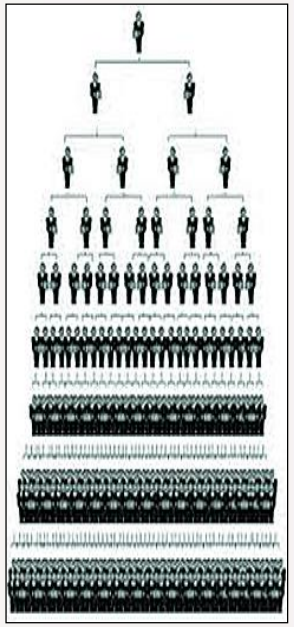
a) Proprietà (TDT)

b) Delegati, Designati (RDT)

c) Soggetti Autorizzati (stagisti temporanei)

d) ADS Interni Resp. Esterni ICT

(ERP/CRM, DAO, Service, HW, CC, Stoccaggi Dati, sito WEB, ecc.)



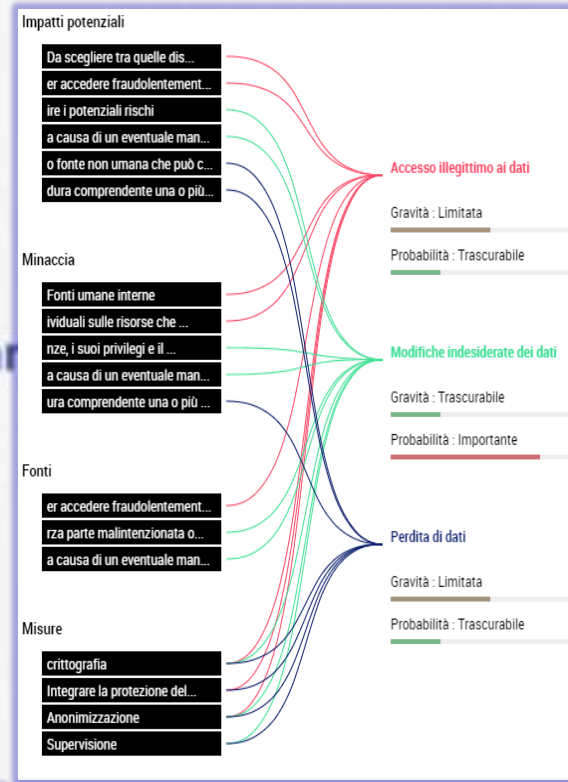
MANUALE SPPD – Reg679/16 SW PER DPIA

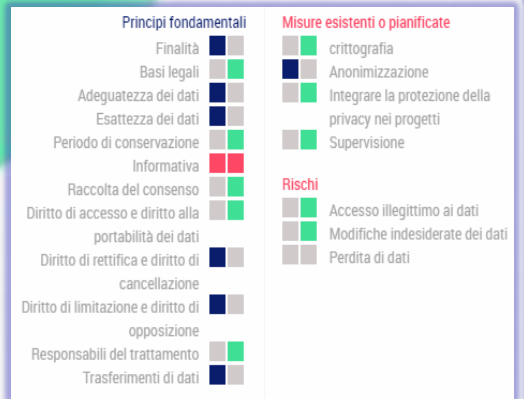
OPEN SOURCE NON VUOL DIRE GRATUITO!

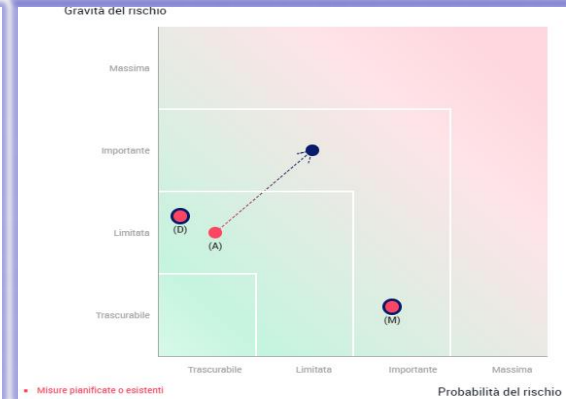
SalvoReina

pia | analyse d'impact sur la protection des donn
privacy impact assessment

NOVITA'
CARTACEO
O
ELETTRONICO







PIA

An overview of the requirements and methodology

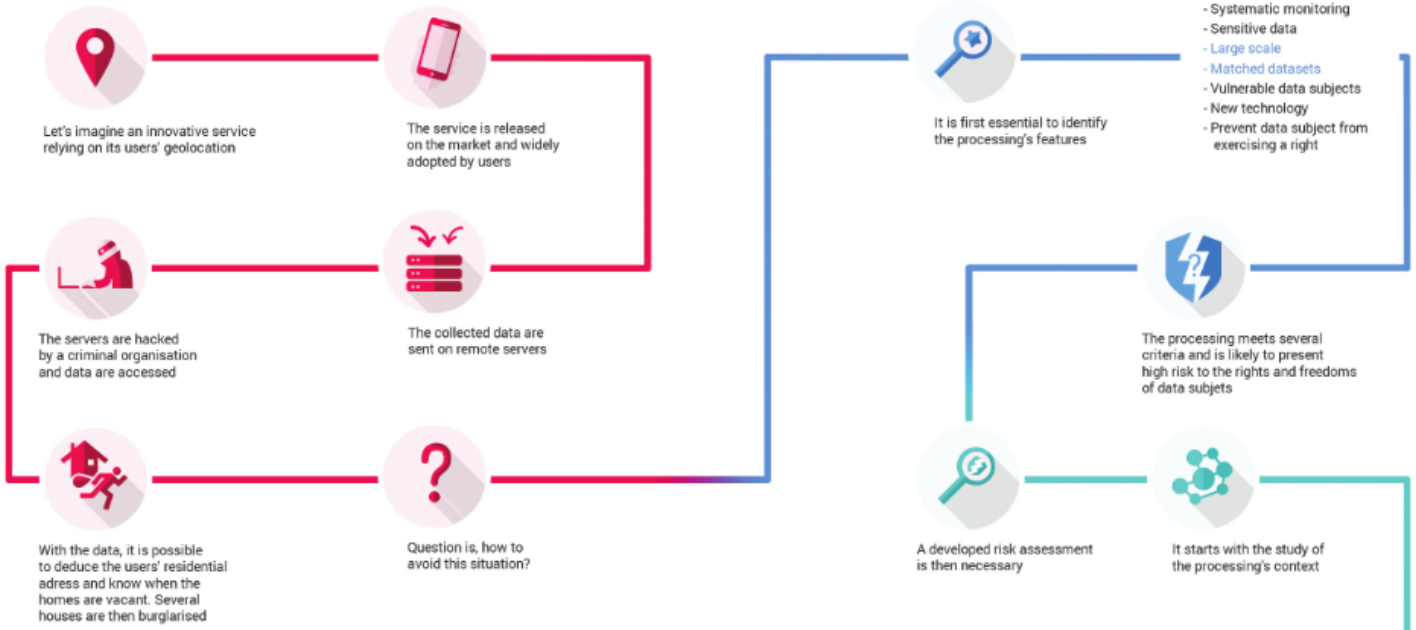
0. Launching a new processing

Every day in the digital realm, numerous services are created.

Those services usually rely on the processing of personal data aiming at fulfilling the needs of organisations or their users.

The supporting assets used to store the data have different levels of vulnerabilities toward feared events such as illegitimate acess, unwanted change, or disappearance of personal data.

Those risks are likely to have significant impacts on the users' privacy.



1. Considering the processing

For the data processor as well as the data subjects, those risks are unwelcome.

Before carrying out a processing, it is essential to analyse it to understand its inherent risks.

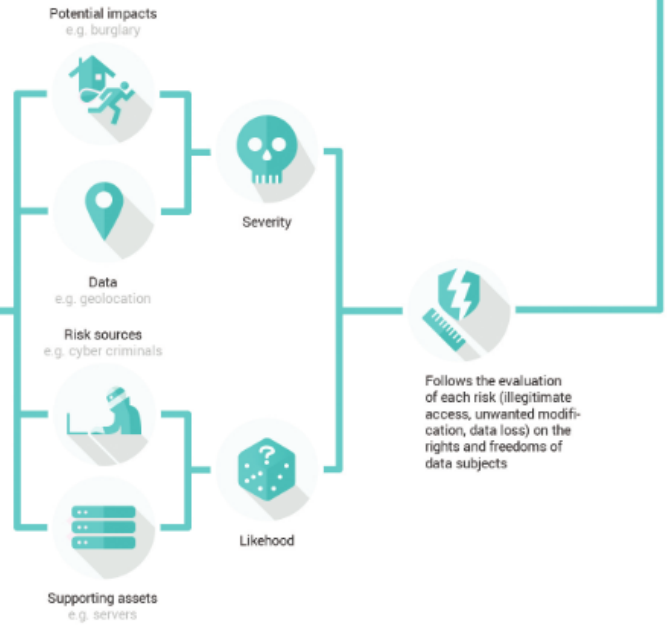
Several factors affect the riskiness of a processing, as the kind of data processed.

Generally speaking, if a processing meets two of the criteria listed, then it is likely to present high risks and would require to carry out a privacy impact assessment.

2. Evaluating the privacy risks

The assessment first establishes the context in which the processing is carried out, including its purpose and technical features.

In addition to studying the fundamental principles, made up of the necessity and proportionality of the processing, each risk has to be analysed to evaluate its severity and likehood according to its potential impacts on the rights and freedoms of data subjects, the data processed, the risks sources and the supporting assets.

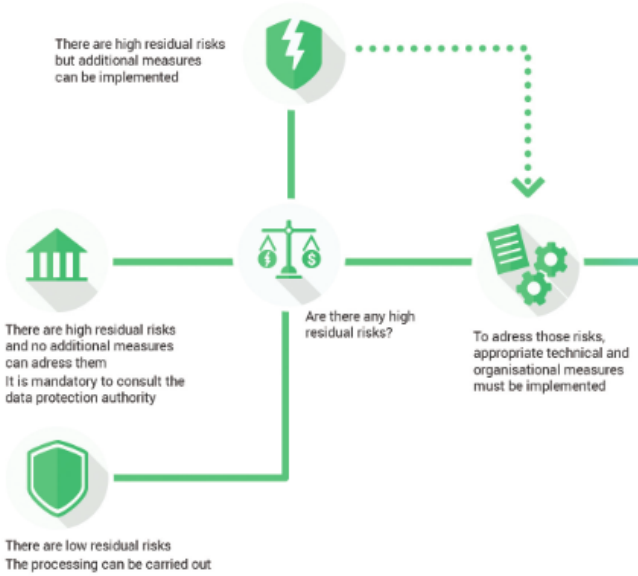


3. Adressing the risks

Once the risks have been identified, it should be determined if they are acceptable given the existing and planned technical and organisational measures.

If it doesn't seem possible in regard of the foreseen measures, the data protection authority has to be consulted.

In any case, it is mandatory to implement the planned controls before carrying out the processing.



MSP è una partita di biliardo a dichiarazione…

General **D**ata
Protection
Regulation

Sistema Qualità e Sicurezza basato su **Governance e Compliance**

Senza **DPO** le organizzazioni faticano e rimangono incerte

PARTE 2

CHI FA E GESTISCE TUTTO IL SISTEMA

- Approccio READINESS
- Ineludibile ruolo DPO/RPD
- Aree critiche e *special topics*

Adattare e Adottare

READINESS !

Non saltate prima di
aver cambiato prospettiva

GDPR e Privacy 4.0: un nuovo paradigma

Privacy Enhancement Tools By ENISA

Uno standard scelto dalla UE

a) Evoluzione della privacy

b) Readiness e *compliance*

Coscienti che la vulnerabilità DP e inversamente proporzionale al successo di business …

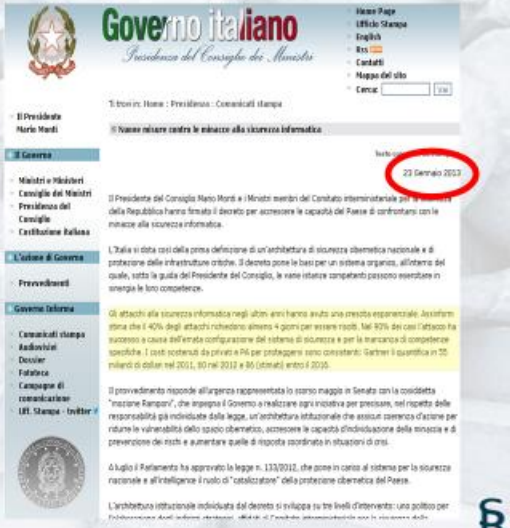
READINESS !

40 % Attacchi costano 4 giorni di stop !

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

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

Pubblico e Privato



EU starts building cyber-response team

Summary: A team will work for a year to set up EU-Cert, a computer emergency response team, for EU institutions including the European Commission, European Parliament and the Council of Europe

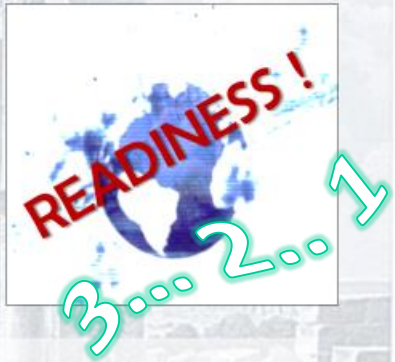
Società del rischio tecnologico globale… Una questione che puzza di UMANO

SUCCEDE SEMPRE AGLI ALTRI !

Rischio digitale di *business* 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**

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 !

Contratto di Intrusione amicale o implicito consulenza DPO

Quanto costa una breccia ?

READINESS !

Comprendere i dati raccolti e prepararsi alla intrusione inevitabile coordinando processi

READINESS !

Conformità <> Compliance

EUROPEAN DATA PROTECTION SUPERVISOR
The European guardian of personal data protection

TOP 15 CONCERNS

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 – Informative/consensi via Portale**
- **Diritto all'oblio – cancellazione definitiva**
- **CLOUD e trattamenti IT (anonimizzazione, conservaz. Sostitutiva, dematerializzazione)**
- **Delocalizzazione e BYOD : ibrido dispositivi privati-aziendali**
- **Contrattualistiche : SLA e accordi di settore – trattamenti con estero**
- **Disciplinare e Policy condivisa con incaricati – superate RSU e DirProvLav**
- Inclusione digitale – Agenda Digitale 2.0
- Misure di backup alter loco : Sito freddo e terzializzazioni IT
- Misure anti frode : furti di identità e preservazione contraffazioni
- Ordini professionali e accordi di settore (AGICOM, ANIA ecc..)

COME DECIDERE: **la PNL del DPO**

READINESS !

Formazione ripensata per la persona in azienda

Dalle piccole cose <–> abitudini ICT virtuose

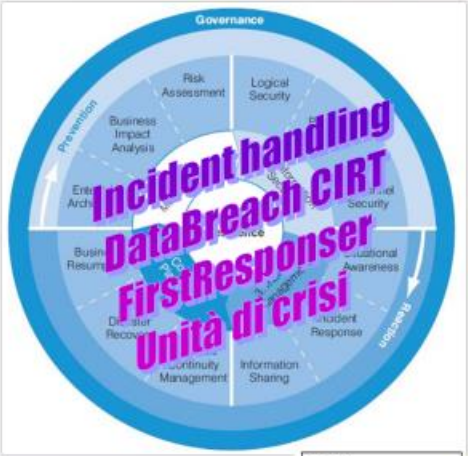
- *Gestione password su smartphone, tablet e portatile*
- *Creare un avviso su Google con il nostro nome*
- *Disconnettere sessioni dei servizi che non usiamo*
- *Non dare pw della propria email*
- *Criptare i dati sul proprio computer se USB/SD*
- *Abilitare la verifica in due passaggi (ES.Gmail)*
- *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*

READINESS !

Dalla Sicurezza alla Resilienza...

Integrazione
Total Quality Management

Non basta la carta.
Il Data Protection traversa sostanzialmente le funzioni aziendali!

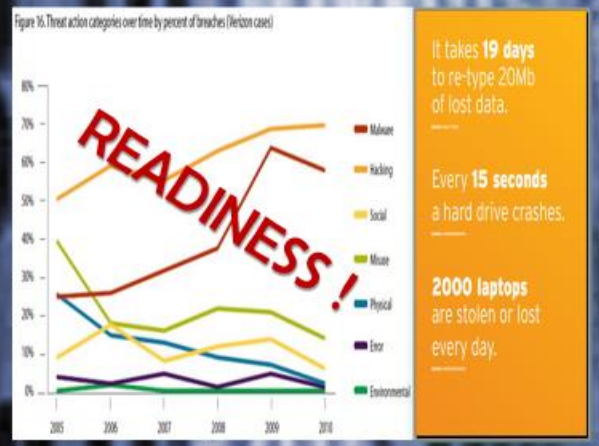


Fonte: Booz&Company, 2011

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.

Privacy 4-0: New Paradigm of **Readiness**

READINESS !

Instrumentare: 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

INSTRUMENTARE - DEMING : Stimare la qualità nera !

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 infettatto e
Quelli che NON sanno di avere un PC infettato

READINESS !

Maggiore fonte di perdità economica !

O DEL LAVORO !!!

Promisquità Inelluttabile irrinunciabile ?

APPLICARE **2FA** PER I **BYOD**

READINESS !

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

La televisione guarderà noi, il lettore multimediale saprà se abbiamo diritto a vedere qualcosa e potrà decidere lui in quale momento farcelo guardare, l'auto sfrutterà il parcheggio per scaricare il software, il forno conoscerà le abitudini alimentari !

DPO

Garante interno

ARTT. 37,38 e 39

Tecnologo di avanguardia: **DPO/RPD**

DPO GUARDA IL 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 . SaasS
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 specchietto retrovisore e al cui sopraggiungere non ci si può sottrarre

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

DPO: FIGURA ACCREDITATA E CERTIFICATA

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

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

DPO: UN CONSIGLIORI DI FAMIGLIA

DPO: IL DESIGNER DELLA PRIVACY BY DESIGN !!!

COME DECIDERE la compliance : trucchi pratici del DPO

Risorse adeguate per il D.P.O.
Normativa privacy nelle attività aziendali DP
adiuva il CDA aziendale (OdV 231/CAD) vinco da Contratto di Consulenza nel Privato e/o Contratto di Servizi Dlg.50/2016 P.A

NON un UFFICIO,

PIUTTOSTO UN TEAM !

Sia nella PA che nel Privato è raccomandabile che il TDT consideri la credibilità del DPO anche se non è richiesta una certificazione al professionista

Requisiti senza Declaratorie !

DPO è la felicità dei legali della organizzazione

Adiuvare il legale della società

… fornisce evidenze forensi utilizzabili

Contenuti proprietari : cugino compiacente porta all'esterno documenti

Litigation : Ricorso per *mobbing* ingiustificato, contrattualistica forniture

Post firing: vendette dopo licenziamento anche non a scopo speculativo (Steganografia)

Cross competition : remore e conflitti con altri dipendenti

Coordinamento giuridico: armonizzare e risolvere incoerenze legislative, scelte strategiche tecnologiche per tutela TDT

ACM DL DIGITAL LIBRARY

The Forensic Analysis of a False Digital Alibi

Authors: Aniello Castiglione, Giuseppe Cattaneo, Giancarlo De Maio, Alfredo De Santis, Gerardo Costabile, Mattia Epifani

2012 Article

Bibliometrics
· Downloads (6 Weeks): n/a
· Downloads (12 Months): n/a
· Downloads (cumulative): n/a
· Citation Count: 0

Published in:
· Proceeding
IMIS '12 Proceedings of the 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing
Pages 114-121
IEEE Computer Society Washington, DC, USA ©2012
table of contents ISBN: 978-0-7695-4684-1 doi>10.1109/IMIS.2012.127

Feedback | Switch to single page view (no tabs)

Abstract | Authors | References | Cited By | Index Terms | Publication | Reviews | Comments | Table of Contents

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

Anche il DPO non idoneo è una violazione!

Perché il DPO è un adempimento!

PROTEZIONE DEI DATI PERSONALI (PRIVACY)

Assistenza ad ogni adempimento previsto da leggi e provvedimenti in materia di privacy.

ANALISI DEI RISCHI

Finalizzata alla IT Governance aziendale ed agli adempimenti obbligatori, quali:

- Art.31 d.lg 196/2003 e DPS

BUSINESS CONTINUITY

Assistenza alla compilazione del Piano di Continuità per i processi critici

PIANI DI SICUREZZA E ICT AUDITING

Compilazione di *Policy* di sicurezza aziendali. sistema di controllo delle principali aree IT

DPO nella organizzazione

Intermediazione di metodi e linguaggi trasversalmente al business
Interfaccia tecnico-regolatoria con l ' IT (logs, email, data retension ecc)

PUNTO DI CONTATTO PER AUTORITA' E INTERESSATI
Nome va pubblicato su WEB (informativa) e comunicato al Garante

DPO

Garante interno

Nelle PP.AA. è più articolato...

ARTT. 37,38 e 39

Perché conviene il supporto di un integratore !

DPO si integra operativamente con le figure P.A.

- Il Responsabile per la transizione alla modalità digitale
- Il Responsabile per la prevenzione della corruzione e per la trasparenza
- Il Responsabile della gestione documentale
- Il Responsabile della conservazione documentale

Art. 17 Cod. Amm. Digitale (IT); Decreto 33/2013 «Trasparenza»; DPR 485/2000 Art.44 C.A.D.
ATTENZIONE: Circ. AGID 2/2017 con scad.31/17

Art. 37, 38 e 39 – DPO / RPD

DPO PPAA: ADEMPIMENTI DOCUMENTI COGENTI

- Il Modello d'implementazione previsto dalla Circolare Agid n. 2/2017 — dal 31/12/2017
- Il Piano di sicurezza del Manuale di gestione documentale e del Manuale di Conservazione — Allegato p. Triennale
- Il Piano di continuità operativa previsto dal Correttivo CAD — dal Dic 2017
- La sezione Trasparenza del Piano triennale per la prevenzione della corruzione

Art. 17 Cod. Amm. Digitale (IT); Decreto 33/2013 «Trasparenza»; DPR 485/2000 Art.44 C.A.D. ATTENZIONE: Circ. AGID 2/2017 con scad.31/17

Art. 38 Comma 1 e 2 – Obblighi TDT/RDT e compiti RPD

Garanzia di autonomia, copertura economica estrumenti per…

- **Informare** e fornire al Titolare, al Responsabile nonché ai dipendenti che eseguono il trattamento, consulenza in merito agli obblighi normativi in materia;
- **Sorvegliare** l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche in materia del Titolare o del Responsabile del trattamento, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa al trattamento e al controllo in merito;
- **Fornire**, se richiesto, pareri sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- **Cooperare** con l'Autorità di controllo;
- **Fungere** da punto di contatto con il Garante per la protezione dei dati di personali per questioni connesse al trattamento.

Anche Interessati Comma 4

Art. 37, 38 e 39 – DPO / RPD

Responsabilità

Il DPO deve essere autonomo ed indipendente:

- non deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati né è soggetto a potere disciplinare o sanzionatorio per l'adempimento dei propri compiti.
- deve avere le risorse necessarie e il potere di spesa per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere le proprie conoscenze specialistiche (es. aggiornamento professionale).

Art. 37, 38 e 39 – DPO / RPD

Competenze, qualifiche e requisiti professionistici

In base all'articolo 37, paragrafo 5, il RPD "*è designato in funzione delle qualità professionali in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*". Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

Certificazioni PA
FAQ Autorità Garante

Art. 37, 38 e 39 – DPO / RPD

DPO Interno nelle PPAA: Nomina o designazione?

- ☑ Nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.
- ☑ Necessario apposito atto di designazione

NON il Segretario Generale dell' ENTE !!!

Art. 37, 38 e 39 – DPO / RPD

DPO Esterno nelle PPAA: incarico a consulente

Il RPD può far parte del personale del titolare o del responsabile del trattamento (RPD interno) ovvero "assolvere i suoi compiti in base a un contratto di servizi". In quest'ultimo caso il RPD sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica. Se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale RPD soddisfi tutti i requisiti applicabili come fissati nel RGPD.

Procedura affidamento: Requisiti, importo, Obbligazioni, e SLA Dlg.vo 50/2016

Art. 37, 38 e 39 – DPO / RPD

DPO PPAA e PRIVATO IN FORMA ASSOCIATA

Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

(art. 37, comma 3, GDPR)

Unioni Comuni (ICT), Amm. sanitarie territoriali Accordi consortili

Art. 37, 38 e 39 – DPO / RPD

DPO PPAA PRIVATO: COMUNICAZIONE ALLA AUTORITA'

- ☑ Comunicazione nominativo RPD e dati di contatto al Garante Privacy
- ☑ Pubblicazione nella sezione "Amministrazione Trasparente" e "Privacy" del sito istituzionale

Interno o Esterno


Aree critiche e Adempimenti Speciali
PRIVACY 4.0 in mare aperto

Privacy 4.0 - Aree-Attività critiche

VDS e statuto lavoratori

Dati e documenti digitali

Compliance organizzativa dati

Gestione Incidenti /violazioni IT

Aree critiche e Adempimenti Speciali

Privacy 4.0 in navigazione

Ano/pseudonimizzazione DB/dockers/VM/clust

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

Job's Act: Telecontrollo lavoratori

Cloud Computing e IoT

Le ispezioni del Nucleo Investigativo Privacy

BIG DATA quanto BIG?

Anonimizzazzione
Minimizzazione
Pseudonimizzazione

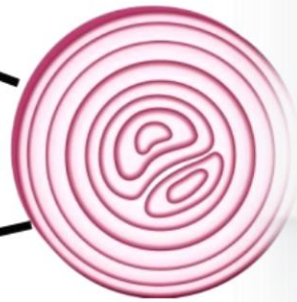
Art. 3 e 4 – Ricorrere anche a «Segmentazione»

Anonimizzazzione
Minimizzazione
Pseudonimizzazione

Gradi progressivi di sforzo per risalire al contenuto in chiaro derivato da DVR/DPIA

MEZZI RAGIONEVOLI

MEZZI IRRAGIONEVOLI



Il dato

Art. 3 e 4 – Linee guida del Garante Europeo 2017-2019

Ricordiamo Art. 3

Minimizzazione (policy non tecnica digitale)

I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità

Misure logiche
Es. Cod. Donaz. Eterol.

A priori secondo ispirazione dei principi By Design e By Default – Precoce senza operazioni sui dati in chiaro

Implicazioni Art. 4.5

Anonimizzazzione

Forma di trattamento orientata a rendere il dato personale anonimo non riconducibile quindi all'interessato

Pseudonimizzazione

Trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative per garantire che i dati non siano attribuiti a una persona identificata o identificabile

Anonimizzazzione
Minimizzazione
Pseudonimizzazzione

Dati Sanitari - eHealth

Pseudonimizzazzione

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

Dal 2015 primi provvedimenti in ambito Telemedicina, RedTech, Clinica e Diagnostica Nosocomiale

Cosa fa HASHING

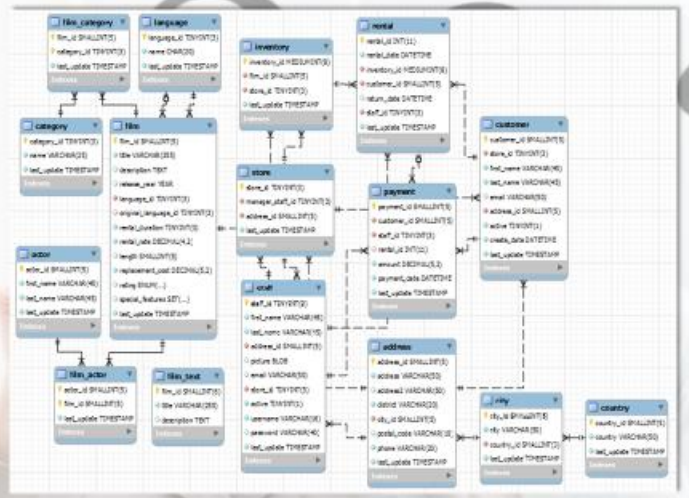
Mario Rossi = a5887a62d652d2b476e57f20bbbc8c2c

Mario Rossi = 9e8999b9d6112271d4ba56aeb463ec1f

Errore comune degli informatici: DEIDENTIFICARE NON VUOL DIRE PSEUDONIMIZZARE

Pseudonomo e distanza del dato dall'interessato

Anonimizzazione e Pseudonimizzazione nei DB



Anonimizzazzione
Minimizzazzione
Pseudonimizzazzione

In sintesi estrema

- Permutazioni orizz. Campi
- Traslocazione ID Tabelle
- Migrazione meta Tabella UID
- Generalizz. Attributi Recs
- Classif. Categoriale
- Posposizione oriz/vert per Honeypot
- Consultivazioni per Marketing
- Sostituz. Valori Aggregati equivalenti
- Cifrature orizzontali chiave/campo
- Copie cifrate di file tabelle (Docker/VM)

Art. 3 e 4 – attenzione alla co-titolarità nel caso di repertori distribuiti condividere meta strutture aleatorie SQL (viste)

Aree critiche e Adempimenti Speciali

Privacy 4.0 in navigazione

Ano/pseudonimizzazione DB/dockers/VM

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

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 !


CYBER-WAR
Ipocrita pensare ad una
difesa totale


Consapevolezza scadente?
Sicurezza e protezione in scadenza!
CYBER-IGNORANCE


CYBER-WAR
Insegnamo resilienza
perché il problema è la
CYBER-IGNORANCE


CYBER-WAR
MANAGERs
PRIVACY 4.0 UNA COSA SERIA
perché non si può fare da soli


REALITYNET
System Solutions
RANSOMWARE

Medical Reputational Disasters

become a supporter | subscribe / find a job

theguardian

news / opinion / sport / arts / life

tech / world / UK / science / cities / global development / business / environment / obituaries

menu

Hacking

Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their files

This article is 1 year old

267 12

Danny Yadron in San Francisco

@dannyyadron

Thursday 18 February 2016 02.37 GMT

'The quickest and most efficient way to restore our systems ... was to pay the ransom,' said Allen S president and chief executive of Hollywood Presbyterian Medical Center. Photograph: Mario Anzuoni

A Los Angeles hospital hit by ransomware swallowed the bitter pill: it pa hackers.

Advertisement

Ad closed by Google

Stop seeing this ad

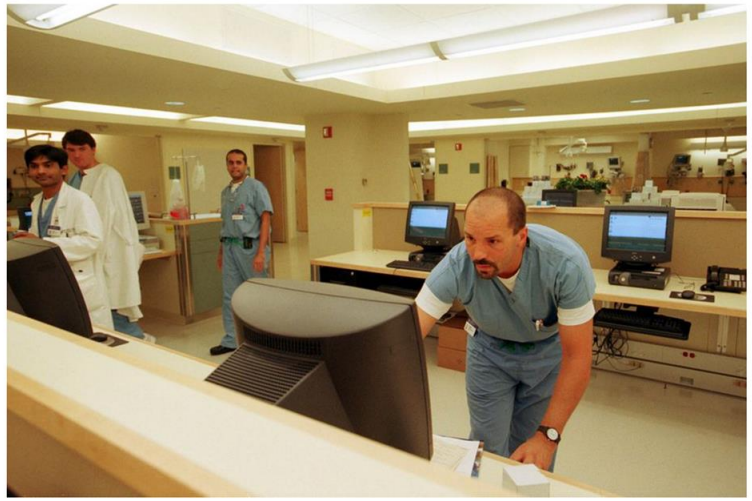
HACKING CYBERSECURITY

U.S. hospitals have been hit by the global ransomware attack

The ransomware is linked to a leaked vulnerability originally kept by the National Security Agency.

BY APRIL GLASER | @APRILASER | JUN 27, 2017, 6:47PM EDT

TWEET SHARE LINKEDIN



Darren McCollester / Getty

Major corporations across the world have been hit by a wave of ransomware attacks that encrypt computers and then demand that users pay $300 to a bitcoin address to restore access.

Ad closed by Google

Stop seeing this ad

AdChoices

TRENDING

TECH CYBERSECURITY

UK hospitals hit with massive ransomware attack

52

Sixteen hospitals shut down as a result of the attack

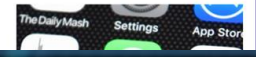
by Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT

SHARE TWEET LINKEDIN

ware attack has shut down work at 16 hospitals across the United g to *The Guardian*, the attack began at roughly 12:30PM local time, d encrypting files. When employees tried to access the computers, they a demand for $300 in bitcoin, a classic ransomware tactic.

NOW TRENDING

Google introduces the feed, a personalized stream of news on iOS and Android



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 può fornire, involont… se informazioni in una mail o rispondendo a…

Si cerca di sfruttare le debolezze de… tura, desiderio di aiuto, …)

Phishing
Brute force
Collasso DDOS
MITM

Endless polymorfism

Beacons traps
Rootkits
Decoys
Breadcrumps
Hijacking
Bouncing
PW mimics
ARP poisoning

Table 1: Traps according to four main types

Files	Network
• Documents (.txt, .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 lmHost files
Applications	**Credentials**
• Session apps (SSH, FTD, 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: Ransomware (20xx)

Protezione euristica – Behavioral Daemon

Minaccia di divulgazione materiale privato

Il ransomware propone "affiliazione" alle vittime

Evoluzione del Social engineering

VEICOLI E TARGET DI ATTACCHI MIRATI

Sicurezza informatica: IL CONTAGIO e-mail

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

Programma contenuto in:

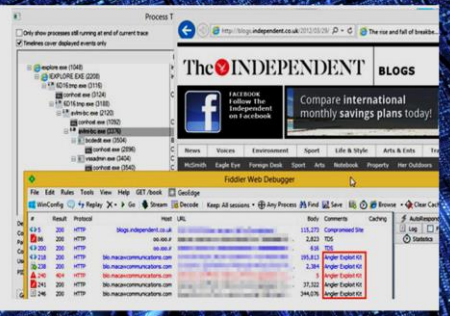
- **Allegato** ad email che parla di fatture, rimborsi, note di credito, spedizioni SDA, etc… anche proveniente da contatti noti
- **Link** alla mail
- Download **da sito web** di finto corriere il cui link è contenuto nell'email ricevuta (spesso su domini realistici oppure di CMS bucati)

Se non si apre l'allegato non si corrono rischi

Sicurezza informatica: IL CONTAGIO web

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

Pericolosi perché non richiedono intervento utente (come aprire mail)



Sicurezza informatica: IL CONTAGIO la RETE

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

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

Sicurezza informatica: IMPATTI ECONOMICI

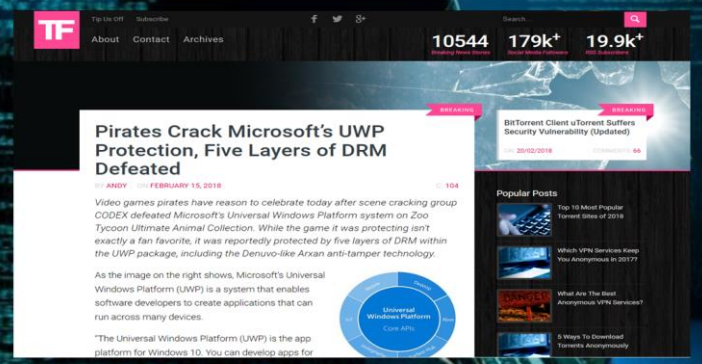
Per la singola infezione:

- ~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 !



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**!

Sicurezza informatica: IL RISCHIO E' CHAT

Telecontrollo lavoratori
Promiscuità BYOD

Adattare al Jobs Act
Sanzionato con la Privacy

Sicurezza informatica: NO GO SOCIAL !!!

Telecontrollo lavoratori
Promiscuità BYOD

Adattare al Jobs Act
Sanzionato con la Privacy

La CYBER-WAR si fa

…con la CYBER-SECURITY

TDT e RDT devono schierarsi !

Aree critiche e Adempimenti Speciali

Privacy 4.0 in navigazione

Ano/pseudonimizzazione DB/dockers/VM

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

Job's Act: Telecontrollo lavoratori

Cloud Computing e IoT

Le ispezioni del Nucleo Investigativo Privacy

Data.Breach
Art. 33

FEDERPRIVACY

Area Riservata

Home Associazione Attività Informazione Strumenti Domande Frequenti

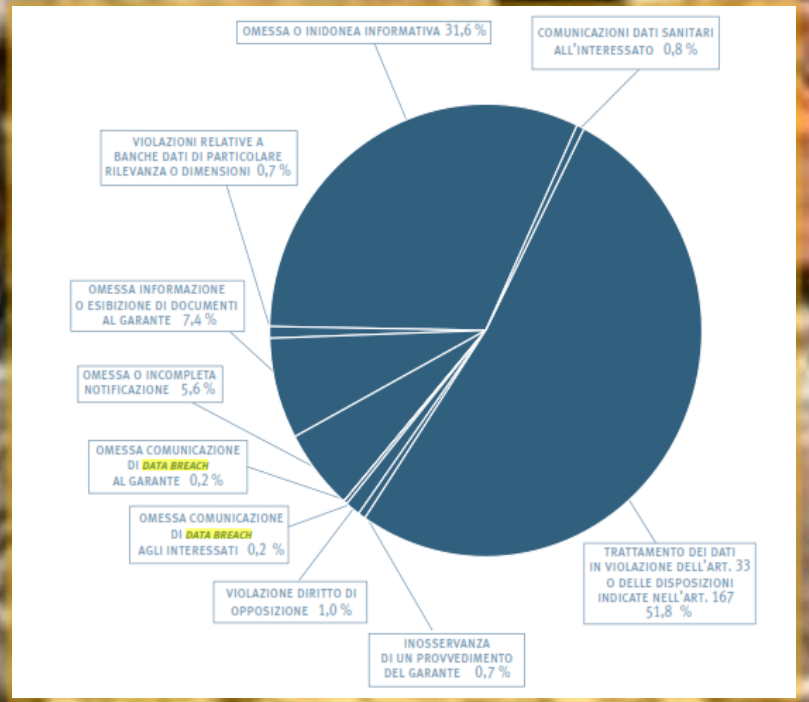
NEWS

Condividi Tweet Condividi Condividi Condividi

Usa, attacco hacker al Pentagono, violati i dati di 30 mila dipendenti

Uno sguardo al mondo Sabato, 13 Ottobre 2018 08:04

Informazioni sui viaggi di 30 mila dipendenti del Pentagono sono state trafugate durante un attacco informatico. A darne notizia è stata una fonte anonima interna all'organizzazione, secondo la quale il numero dei dati compromessi sarebbe destinato a crescere, secondo quanto riferito dalla Cnbc. I pirati informatici sono riusciti a introdursi nei sistemi di un fornitore esterno del Pentagono, al quale hanno sottratto identità, dati delle carte di credito e informazioni di viaggio di civili e militari dipendenti dell'organizzazione.



Health care Data Violation Reality

TREND MICRO | SIMPLYsecurity

Search:

Latest Posts | Categories | Our Experts | Research

Home » Industry News » Current News » Healthcare provider hit by advanced persistent threat: Protecting client information

Healthcare provider hit by advanced persistent threat: Protecting client information

Posted on: September 13, 2014 Posted in: Current News, Industry News, Vulnerabilities & Exploits
Posted by: Trend Micro

In mid-August, healthcare provider Community Health Systems announced that its computer system had fallen victim to an attack. The security incident, which took place in April and June, was an external criminal infiltration by an advanced persistent threat group based in China, The Wall Street Journal reported.

Community Health Systems, which operates 206 hospitals across 29 states, consulted cybersecurity firm Mandiant after discovering the attack. The data protection company determined that the likely cause of the attack was the advanced persistent threat organization. The group reportedly leveraged a considerably sophisticated malware sample to breach the healthcare provider's internal systems.

The infection allowed hackers to sidestep all security measures present on Community Health Systems' infrastructure, enabling them to copy and transmit sensitive information to an outside receiver. The data compromised in the attack includes the names, addresses, birthdates, phone numbers and Social Security numbers of the hospitals' patients. While no financial information was breached, the details transmitted by hackers are more than enough to commit a whole host of fraudulent activities, including those connected with identity theft.

SECURITY INTELLIGENCE BLOG

- ProMediads Malvertising and Sundown-Pirate Exploit Kit Combo Drops Ransomware and Info Stealer
- Linux Users Urged to Update as a New Threat Exploits SambaCry
- Android Backdoor GhostCtrl can Silently Record Your Audio, Video, and More

FEATURED AUTHORS

Dustin Childs (Zero Day Initiative Communications)

Ed Cabrera (Chief Cybersecurity Officer)

DON'T MISS: How to expose flaws in custom-built mobile apps · How Google's Chrome browser does updates · IDG Enterprise's Digital Edge 50 · Resources/White Papers

COMPUTERWORLD FROM IDG

INSIDER Sign In | Register

CenturyLink Business — Moving to a More Efficient Cybersecurity Strategy — EXPAND

Home > Vertical Industries > Health Care

NEWS

Update: Hacker puts 9.3M U.S. patient records up for sale

The hacker claims to have already sold $100,000 worth of records

By Lucas Mearian
Senior Reporter, Computerworld | JUN 28, 2016 2:54 PM PT

MASSACHUSETTS GENERAL HOSPITAL

Conditions & Treatments | Centers & Departments | Education & Training | Research

Find a Doctor
Find a Researcher
Appointments & Referrals

‹ Mass General News

News Release

Wednesday, June 29, 2016

Massachusetts General Hospital notifies patients of a privacy incident at a third-party vendor

BOSTON – Massachusetts General Hospital (MGH) announced today that it is notifying individuals related to a privacy incident involving information stored by a third-party vendor. The incident did not involve information that was stored or maintained on MGH's systems.

Patterson Dental Supply Inc. (PDSI) is a trusted third-party vendor that provides software that helps manage dental practice information for various providers, including MGH. On February 8, 2016, MGH learned that an unauthorized individual gained access to electronic files used on PDSI's systems, and later confirmed that the files contained some MGH dental practice information. PDSI reported the incident to law enforcement. Thereafter, law enforcement investigators required that any notification to potentially affected individuals and any public announcement of the incident should be withheld while they were conducting their investigation. On May 26, 2016, law enforcement gave permission to notify, and MGH began this notification as quickly as possible once the hospital had completed its investigation.

Contact Public Affairs

Connect with Mass General

Sei in: Repubblica Milano / Cronaca / Trivulzio, attacco informatico ...

IL CASO

Tweet | Consiglia 566

Trivulzio, attacco informatico "Hanno cancellato gli archivi"

A Ferragosto un presunto hacker ha manomesso i computer. Il misterioso episodio denunciato alla polizia postale. Persi rendiconti finanziari e documentazione sanitaria

di FRANCO VANNI

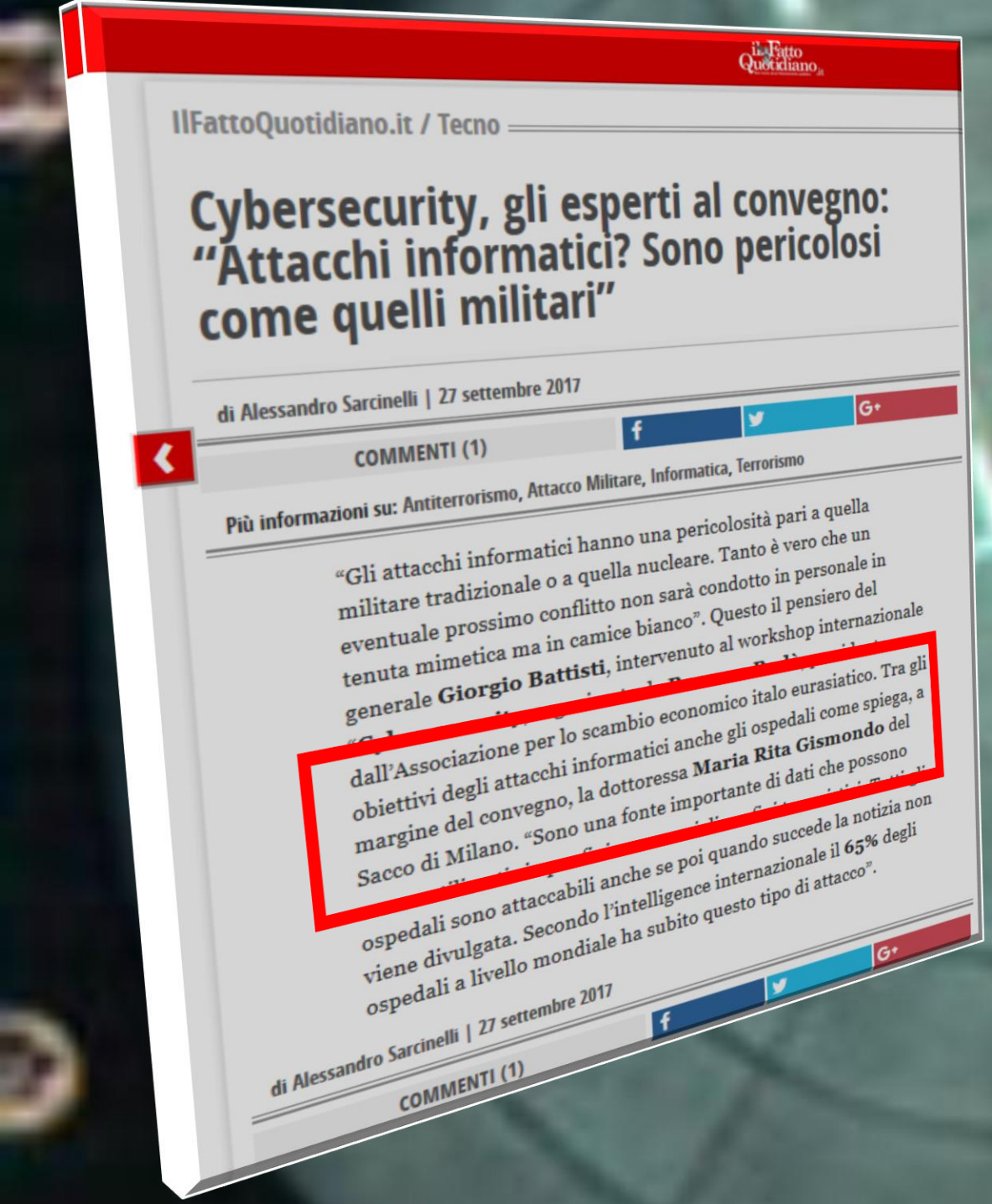
Quarantotto ore per cancellare tutto. Due giorni per ripulire dai dati la rete informatica del Pio Albergo Trivulzio. L'attacco informatico è scattato a Ferragosto, con gli uffici chiusi. Dai pc e dai server della casa di riposo sono stati fatti sparire i documenti relativi alla contabilità, le schede cliniche dei pazienti, l'elenco del personale, i moduli di pagamento, l'agenda delle prenotazioni delle visite e tutto quello che riguarda il patrimonio immobiliare. La direzione del Pat ha fatto denuncia alla polizia postale, che su mandato della Procura indaga sull'autore e sulle motivazioni del blackout. Non si esclude che chi ha cancellato i dati abbia prima potuto copiarli. La Procura ha aperto un'inchiesta (al momento a carico di ignoti) per accesso abusivo a sistema informatico aggravato e danneggiamento informatico.

Chi è entrato nella memoria informatica del Pat aveva come obiettivo quello di distruggere. File e documenti di ogni tipo sono stati bruciati e anche gli archivi informatici "di riserva", la "backup memory", sono stati ripuliti. Gli agenti della Postale, che al Trivulzio avrebbero già fatto un'ispezione, cercano di recuperare il recuperabile grazie a tecniche sofisticate. La speranza è che dietro ai monitor privi di immagine si facciano riaffiorare i documenti che raccontano il presente e la storia recente del Pat. Di certo, chi ha agito sapeva cosa fare. L'ipotesi più probabile è che il pirata informatico sia entrato in decine di computer "da remoto", collegandosi tramite la rete. Ma non si esclude che per manomettere i computer qualcuno possa essersi fisicamente introdotto nell'edificio.

400 Bad request

Your browser sent an invalid request.

65% di Nosocomi e strutture sanitarie Bersagli informatici



IlFattoQuotidiano.it / Tecno

Cybersecurity, gli esperti al convegno: "Attacchi informatici? Sono pericolosi come quelli militari"

di Alessandro Sarcinelli | 27 settembre 2017

COMMENTI (1)

Più informazioni su: Antiterrorismo, Attacco Militare, Informatica, Terrorismo

"Gli attacchi informatici hanno una pericolosità pari a quella militare tradizionale o a quella nucleare. Tanto è vero che un eventuale prossimo conflitto non sarà condotto in personale in tenuta mimetica ma in camice bianco". Questo il pensiero del generale **Giorgio Battisti**, intervenuto al workshop internazionale dall'Associazione per lo scambio economico italo eurasiatico. Tra gli obiettivi degli attacchi informatici anche gli ospedali come spiega, a margine del convegno, la dottoressa **Maria Rita Gismondo** del Sacco di Milano. "Sono una fonte importante di dati che possono ospedali sono attaccabili anche se poi quando succede la notizia non viene divulgata. Secondo l'intelligence internazionale il **65%** degli ospedali a livello mondiale ha subito questo tipo di attacco".

di Alessandro Sarcinelli | 27 settembre 2017

COMMENTI (1)

Maria Rita Gismondo S.C: Lab.Microb. Clinic. Polo Univ. A.O. "L. Sacco" di Milano

Gen. C.A. Giorgio Battisti NATO Defence College Foundation

Data.Breach Art. 33 coordinato disposto

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

Data.Breach Art. 32

Adempimenti

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

Art. 32-bis(((Adempimenti conseguenti ad una violazionedi dati personali)))
((1. In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili 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 contraente o di altra persona, il fornitore 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 fornitore non vi abbia gia' provveduto, il Garante puo', considerate le presumibili ripercussioni negative della violazione, obbligare lo stesso a comunicare al contraente o ad altra persona l'avvenuta violazione.
5. La comunicazione al contraente 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 fornitore per porvi rimedio.
6. Il Garante puo' emanare, con proprio provvedimento, orientamenti e istruzioni in relazione alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonche' alle relative modalita' 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

Data.Breach

Procedura DP Autorità

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

Aree critiche e Adempimenti Speciali

Privacy 4.0 in navigazione

Ano/pseudonimizzazione DB/dockers/VM

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

Job's Act: Telecontrollo lavoratori

Cloud Computing e IoT

Le ispezioni del Nucleo Investigativo Privacy

Video Sorveglianza eTelecontrollo

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 alcunchè rimanda Diritto Nazionale sul Lavoro Art. 88

Video Sorveglianza eTelecontrollo

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

Video Sorveglianza eTelecontrollo

DP : Non solo telecamere

Gli impatti dell'art. 4 S.L.

- Videosorveglianza e droni;
- GPS sui mezzi assegnati ai dipendenti;
- Accessi biometrici;
- BYOD e log di connessione alla rete aziendale tramite dispositivi personali;
- MDM;
- IoT;
- Proxy (filtraggio della navigazione e black list);
- Antivirus;
- Log di connessione alla posta elettronica aziendale;
- VPN;
- Log del sistema operativo;
- Log di accesso a stampanti e scanner;
- Sistemi di registrazione accessi fisici ad aree aziendali;
- Software per call-center;
- Dati relativi al traffico telefonico e software per il monitoraggio costi;
- Software che tracciano accesso a cartelle;
- Altri casi

Ricordiamo L'Interpello ex Art. 17

Video Sorveglianza eTelecontrollo

DP : controllo a distanza

Controllo a Distanza si intende non solo nella accezione fisica geografica ma di Tempo !!!

Si pensi al controllo dei Log

La sanzione Lavoristica sta nel codice DP

Video Sorveglianza Telecontrollo

DP dei Lavoratori ai tempi del Jobs Act

Nuovo art. 4 - Comma 1
Jobs Act e Tecnocontrolli

«1. Gli **impianti audiovisivi** e gli **altri strumenti** dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente **per esigenze organizzative e produttive,** per **la sicurezza del lavoro** e per la **tutela del patrimonio aziendale** ...

Adesso ispirazione per allineare e adeguare la pressione tecnologica

Video Sorveglianza Telecontrollo

DP impatto sui Lavoratori ai fini DPIA

Cass. Pen. 22611/2012

"Non integra il reato previsto dall'art. 4 dello Statuto dei lavoratori l'installazione di un sistema di videosorveglianza potenzialmente in grado di controllare a distanza l'attività dei lavoratori, la cui attivazione, anche in mancanza di accordo con le rappresentanze sindacali aziendali, sia stata preventivamente autorizzata per iscritto da tutti i dipendenti"

Secondo la Suprema Corte, "*se è vero - come è innegabile - che la disposizione di cui all'art. 4 intende tutelare i lavoratori contro forme subdole di controllo della loro attività da parte del datore di lavoro e che tale rischio viene escluso in presenza di un consenso di organismi di categoria rappresentativi (RSU o commissione interna), a fortiori, tale consenso deve essere considerato validamente prestato quando promani proprio da tutti i dipendenti*".

Garanti UE: 9 casi pratici per bilanciare Interesse Legittimo e Nuove Tecnologie IT

Video Sorveglianza Telecontrollo

DP dei Lavoratori ai tempi del Jobs Act

Nuovo art. 4 – Comma 2
Gli strumenti utilizzati dal lavoratore

2. La disposizione di cui al primo comma non si applica agli strumenti utilizzati dal lavoratore **per rendere la prestazione lavorativa** e agli strumenti di registrazione degli accessi e delle presenze.

Biometria per accesso CED
GeoLocalizz Spazzaneve o rifiuti

Comma 2 nuovo Art. 4 del Jobs Act – strumenti funzionali al lavoro

Video Sorveglianza Telecontrollo

DP dei Lavoratori ai tempi del Jobs Act

Nuovo art. 4 - Comma 1
Utilizzabilità delle informazioni raccolte

3. Le informazioni raccolte ai sensi del primo e del secondo comma sono utilizzabili **a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196**».

Espresso richiamo alla Privacy; e premia il TDT coraggioso !

Aree critiche e Adempimenti Speciali

PrivaCY 4.0 in navigazione

Ano/pseudonimizzazione DB/dockers/VM

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

Job's Act: Telecontrollo lavoratori

Cloud Computing e IoT

Le ispezioni del Nucleo Investigativo Privacy

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

I vantaggi sono chiari parliamo dei problemi di contrattualità

Public, Private and Hybrid

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

Chi è il TDT e il proprietario ?

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

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

CSA Italy Chapter cloud security alliance℠

Mind Map di ENISA

IoT

Dangerous

By Design By Default!!!

In attesa del 5G, arrivano le pillole smart telecomandate e robotizzate, l'IA, i big data, i farmaci "edibles", le soluzioni RFID e l'automazione, la telemedicina: così i nostri ospedali si fanno

IoT Medical Devices Hacking

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FORUMS

SCIENTIFIC METHOD —

Hacking implanted defibrillators: shockingly easy

Researchers find that implanted cardiac defibrillators, which shock the heart ...

JOHN TIMMER - 3/12/2008, 6:57 PM

Implanted medical devices are becoming increasingly sophisticated, moving from simple pacemakers to computerized devices that can actively respond to changes in a patient's condition. Perhaps the most sophisticated devices commonly in use are implanted defib... These devices monitor the heart's electrical activity and, when an arrhythmic event is de...

WIRED Hacker Can Send Fatal Dose to Hospital Drug Pumps

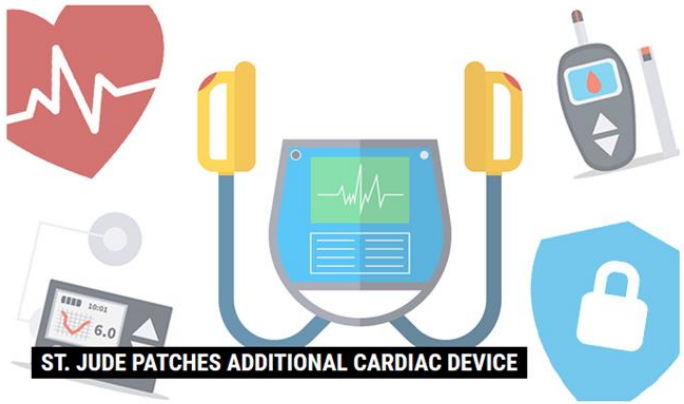
KIM ZETTER SECURITY 06.08.15 07:00 AM

HACKER CAN SEND FATAL DOSE TO HOSPITAL DRUG PUMPS

Hospira's drug infusion pumps include a serial cable (the wide grayish-white cable with the single red stripe on one edge) that connects the communications module to the main pump board. BILLY RIOS

threatpost CATEGORIES FEATURED PODCASTS VIDEOS

Welcome > Blog Home > Cryptography > St. Jude Patches Additional Cardiac Device



by Tom Spring February 7, 2017 , 1:15 pm

St. Jude Medical has patched a vulnerability in another Merlin@home Transmitter medical device vulnerable to a man-in-the-middle attack.

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME ABOUT ICSJWG INFORMATION PRODUCTS TRAINING FAQ

Alert (ICS-ALERT-13-164-01) More Alerts

Medical Devices Hard-Coded Passwords

Original release date: June 13, 2013 | Last revised: October 29, 2013

Print Tweet Send Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

SUMMARY

Researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices exploited to potentially char...

Because of the critical and ... with the Food and Drug Ad... affected vendors of the repo... ICS-CERT is issuing this al... these and other cybersecur... appropriate...

Excuse me while I turn off your insulin pump

DEAN TAKAHASHI @DEANTAK AUGUST 4, 2011 4:58 PM

Diabetics beware. It is possible to hack your insulin pump, from a distance, so that it can harm you rather than save your life. Other medical devices are also vulnerable to hacking in the current age of cyber insecurity. As if patients don't have enough to worry about.

In a talk at the Black Hat security conference in Las Vegas, Jerome Radcliffe, a diabetic himself and a security researcher, showed how he figured out how to hack into insulin pumps for diabetics.

VB Recommendations

Telltale announces The Walking Dead's final season plus new seasons of Batman and The Wolf Among Us

Nimble Named #1 in Sales Intelligence Customer Satisfaction and High Performer by G2 Crowd

Nokia phone maker HMD Global

Aree critiche e Adempimenti Speciali

PrivaCY 4.0 in navigazione

Ano/pseudonimizzazione DB/dockers/VM

CyberWAR, CyberSec, CyberSpace e DP

Data Breach – cosa è, e come si affronta

Job's Act: Telecontrollo lavoratori

Cloud Computing e IoT

Le ispezioni del Nucleo Investigativo Privacy

ISPEZIONI DATA PROTECTION E PRIVACY

Rapporto del Garante (nel primo anno *2010-11*)

- **Ispezioni** : 230 ispezioni, 181 procedimenti sanzionatori, 13 violazioni penali
- **Omesse** : informativa, notificazione, misure idonee, nomine/deleghe ADS
- **Mancati adempimenti** : provvedimenti, adeguamenti comunque cogenti
- **Ambiti** : investigazioni, assicurazioni, sanità, profilazione Cent.Rischio, telemarketing, sharing economy, Agenzie e istituti di Statistica, intermediazione creditizia
- **Comminazioni** : 3 milioni 234 mila € in 15 mesi (41-53 segnalaz Autorità Giudiziaria)

Intanto il bilancio 2017 dell'attività ispettiva dell'Autorità conferma il forte incremento dell'attività sanzionatoria già registrata lo scorso anno. Nel corso del 2017 sono stati infatti definiti oltre 1.000 procedimenti sanzionatori in più rispetto all'anno precedente, pari ad un aumento del 307%. L'importo della sanzioni applicate con ordinanza-ingiunzione sono cresciute arrivando ad oltre 13 milioni e 300 mila euro. Le sanzioni già riscosse dall'erario sono state di circa 3 milioni e 800 mila euro (pari ad un complessivo 15% in più rispetto al 2016).

Cosa è il GAT ?

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

Propone solamente alla Autorità Garante!

PROTOCOLLO DI INTESA

ISPEZIONI DATA PROTECTION E PRIVACY

Cosa è il GAT ?

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

Dal Gen Rapetto >> Cmd.

Col. Menegazzo >> Col. Reccia

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.***

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 cosi da realizzare ispezioni sistematiche secondo settori merceologici

Le pattuglie sono le stesse che controllano gli scontrini!

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

Composizione della pattuglia: **Ispezione preventiva**

1. **Due finanzieri**
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-scanzione 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 Apparati 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!

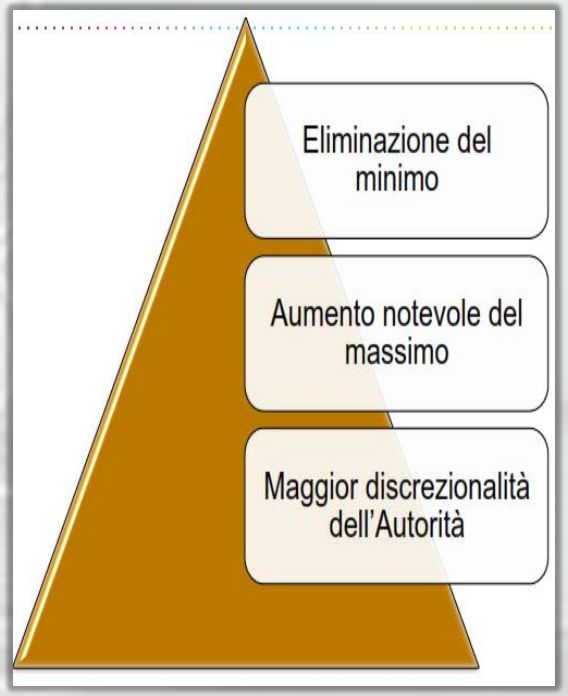
PRIVACY 4.0: Controllo anche via **Call Center**

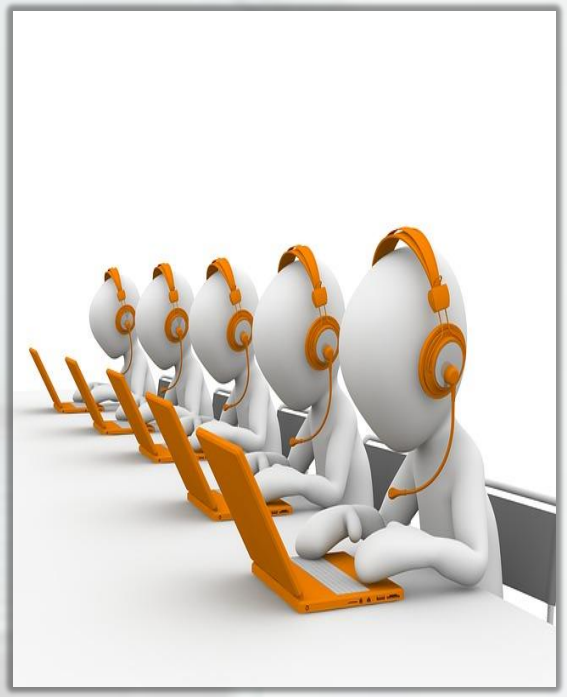
Sanzioni civili, penali e amministrative...

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





Regolamento Europeo ⇨ INVERSIONE DELL'ONERE DI PROVA Art. 2050

PRIVACY 4.0: Controllo anche via Call Center

Sanzioni civili, amministrative e penali...

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 contitolarità (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
- Omesse informazioni all'Ente di Certificazione
- Violazioni degli Organismi di Certificazione

Regolamento Europeo

Sanzioni civili, amministrative e penali

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

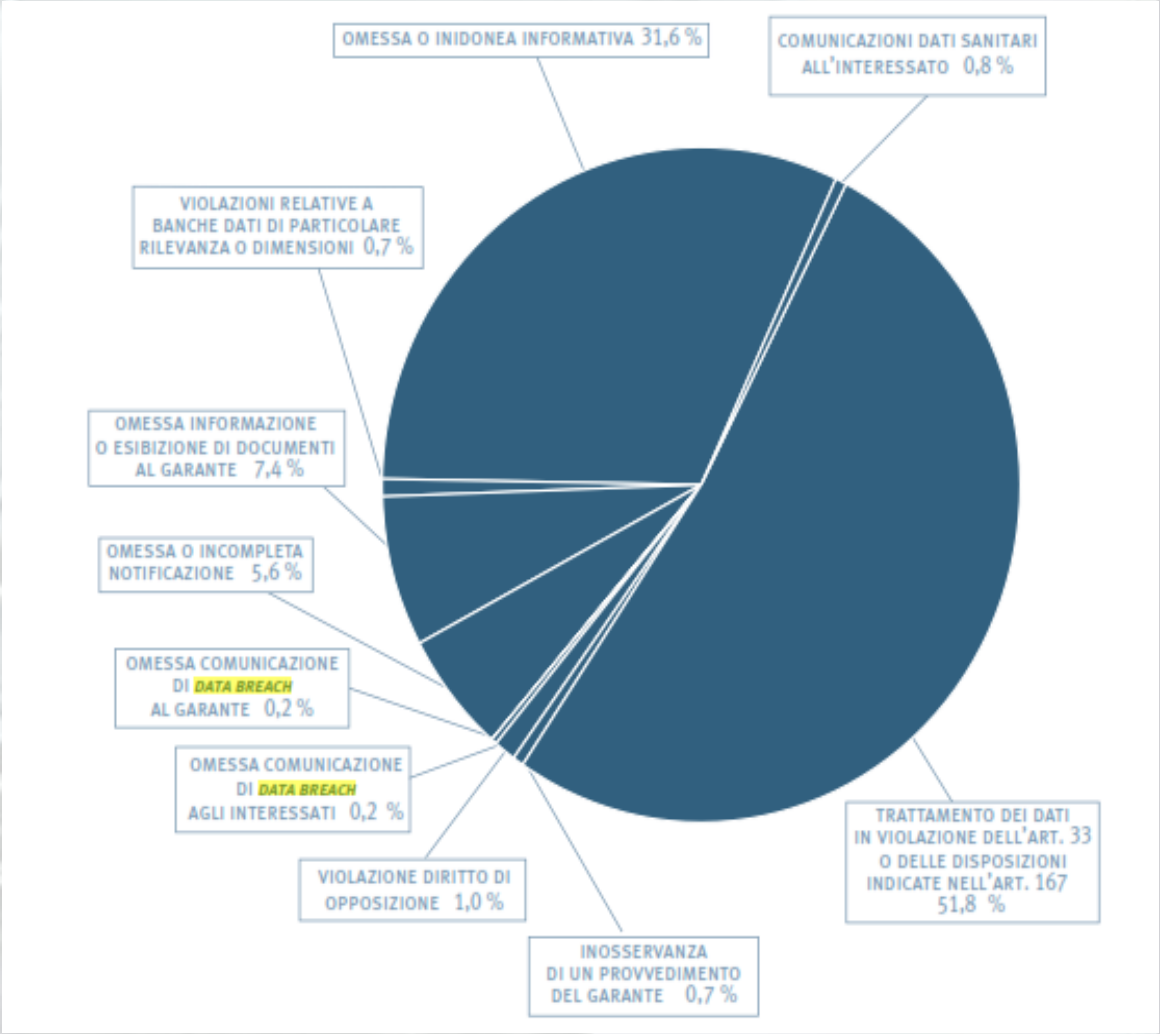
- per violazione ai principi base del trattamento
- per violazione dei diritti dell'interessato (*cancellazione, portabilità etc…)*
- per violazioni su trasferimenti a paesi extra EU
- Violazioni ad obblighi introdotti da Stati Membro
- Inosservanza delle prescrizioni/inibizioni dell'Autorità ai sensi dell'art. 58

Giurisdizione

Competenza Amministrativa → Stato di abituale dimora/lavoro dell'interessato
ART.77
Stato ove si è verificata la violazione (residuale)

Competenza Giurisdizionale → Stato ove ha sede il Titolare o il *processor*
ART.79
Stato ove ha sede l'interessato (residuale)

Applicazione del principio del *ne bis in idem* (art.81) con sospensione



Regolamento Europeo

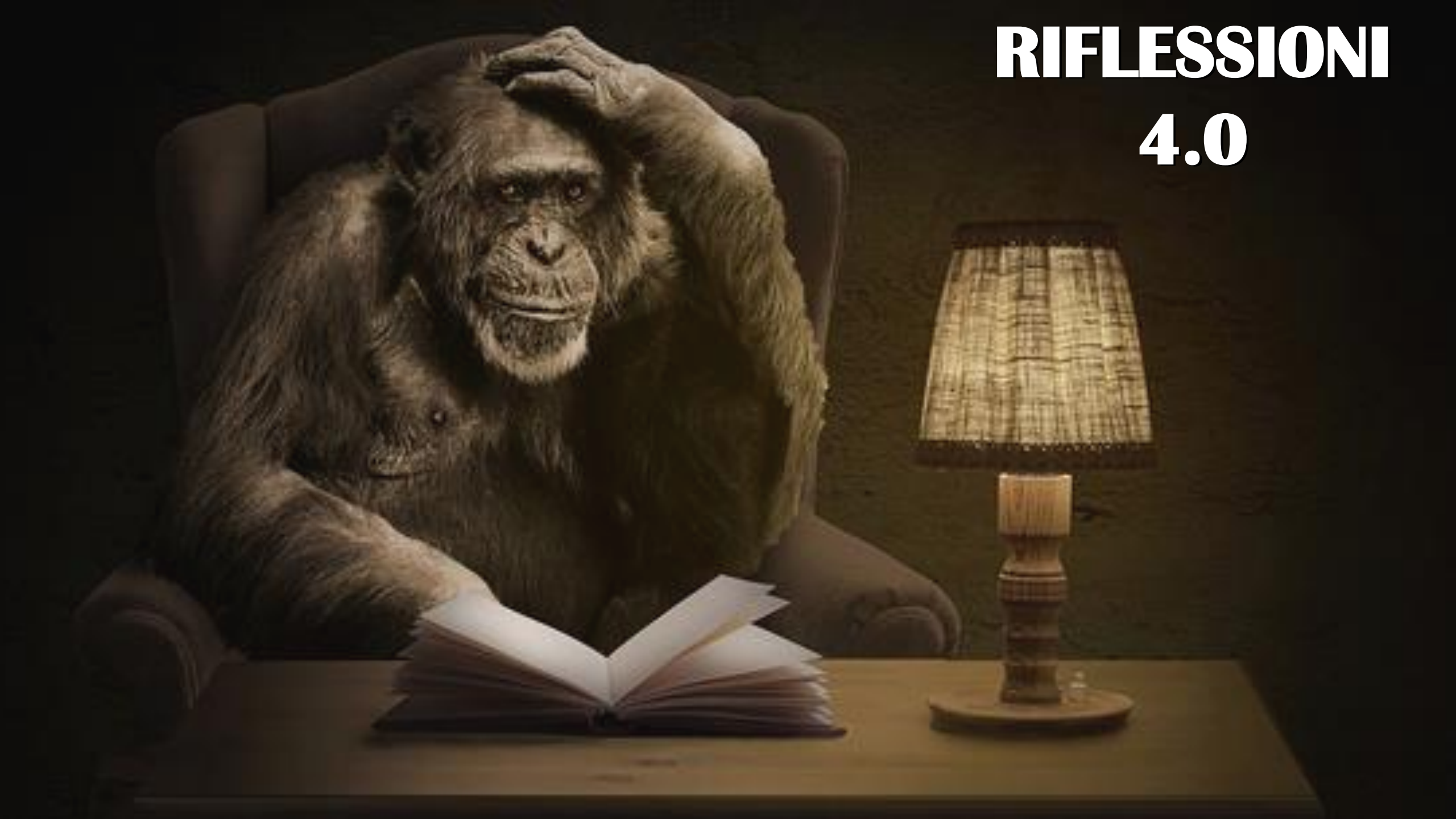
Privacy 4.0 : SANZIONATO L'ATTEGGIAMENTO

Controlli: astenersi da panòplia – Dlg.101/2018

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

Verso il Question Time…

Privacy 4.0 nella PMA


RIFLESSIONI
4.0

APPROCCIO 4.0

Non necessariamente dobbiamo essere geni che conoscono la relatività e la materia oscura!

Il salto quantico non è possibile senza :

- **Commitment proprietà**
- **sistema deleghe forte**
- **un DPO professionale**

… atterrate in sicurezza…


New Mindset:
NON HO TEMPO


Non si migliora
quello che non vedi

Non usate manuali nel *deep web*


Non confondere
Sforzi con risultati !

«Tutto» il possibile, non il «minimo» possibile

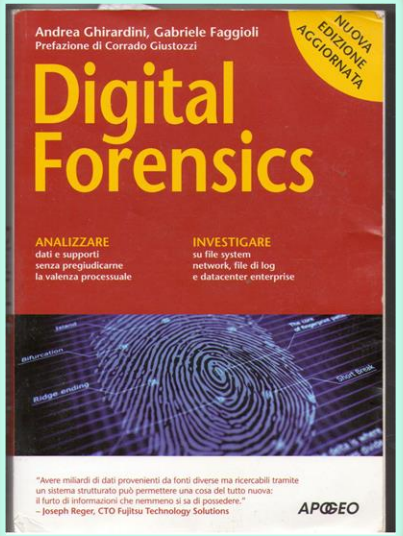
Responsabili PMA come Leadership coaching «Enactment» (Karl Kleick)

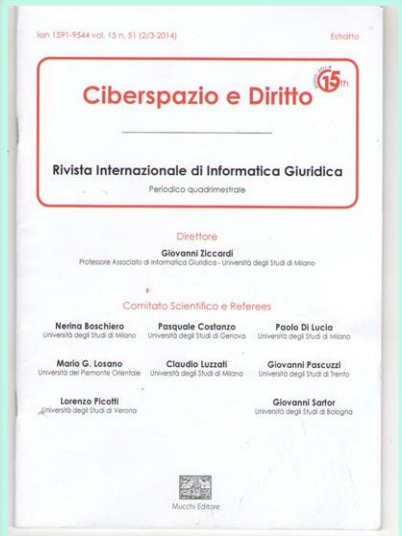
L’approccio fai da te poco plausibile …

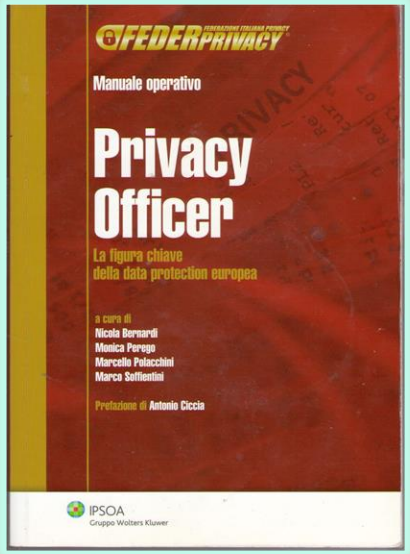

Possibile
ricomprare
tutto
Tecnologia,
Uffici,
Personale …
Non i tuoi Dati

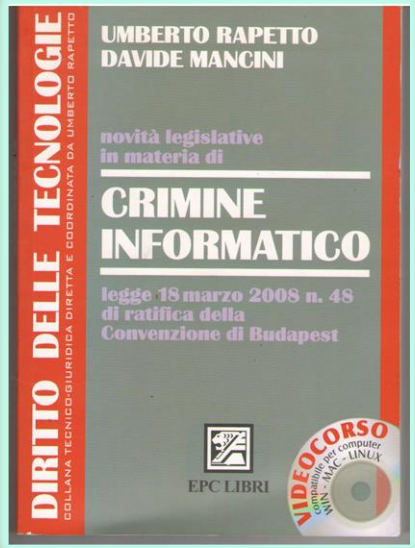
Non rimandare…

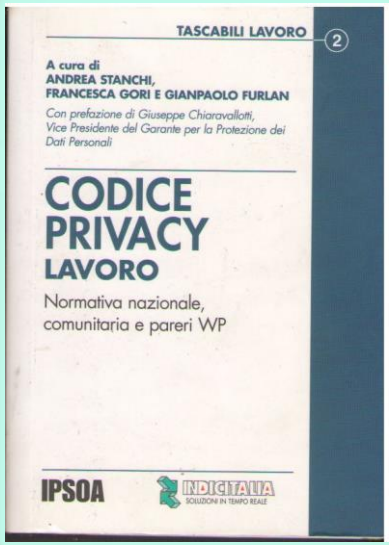

Se non vi occupate di Privacy
lei si occuperà di voi!

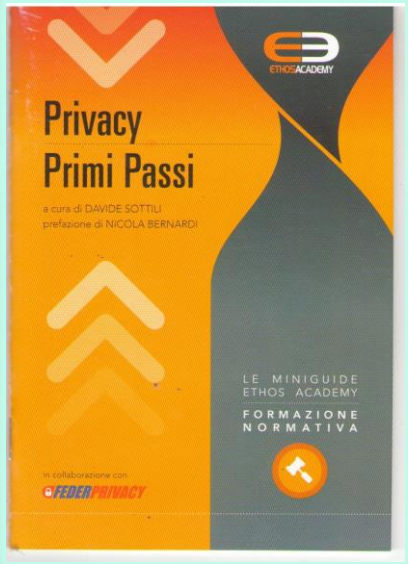


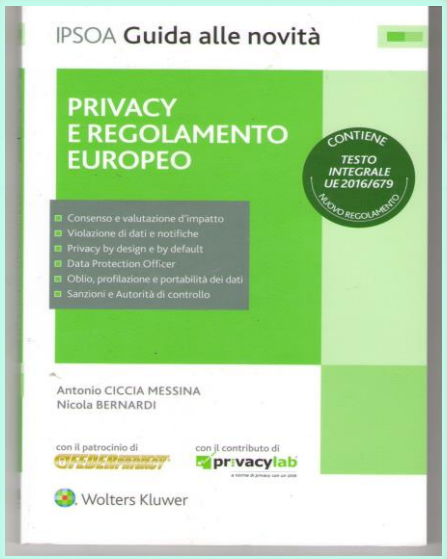












NET FOR LEGAL

FEDERPRIVACY FEDERAZIONE ITALIANA PRIVACY

NIST National Institute of Standards and Technology U.S. Department of Commerce

European Commission

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NATIONAL PRIVACY COMMISSION

Egr. Sig.
Salvatore Reina
Corso Solferino
16122, Genova

Oggetto: Dichiarazione

Con la presente si attesta che il sig. Salvatore Reina, C.F. RNESVT60A10C342J, n° registro CDP_041, ha positivamente superato l'iter di certificazione in accordo allo schema CDP "Consulente della Privacy e Privacy Officer" in data 27/07/2012.

Per l'Organismo di Certificazione TÜV Italia Srl

Luca Boniardi
Responsabile Qualità e Accreditamenti

Result paper

SALVO REINA

Utrecht, 7 July 2010

EXIN hereby certifies that SALVO REINA has participated in the examination

BIL® V3 Service Strategy

on 16-06-2010 and has

Passed

with a score of 29 points

Coaching report

M.R.B. van der Lande
CEO EXIN

exin

This is to certify that

Salvo Reina

has passed the

ITIL® V3 Intermediate Qualification:
Service Strategy
Certificate

16-06-2010

M.R.B. van der Lande
CEO EXIN

EXIN
Examination Institute for Information Science

ITIL
APM GROUP
OGC

00155236

AFGE Alta Formazione Giuridico-Economica

FORMAZIONE

TAVOLA ROTONDA ISTITUZIONALE

IL RESPONSABILE DEI DATI PERSONALI NEL NUOVO REGOLAMENTO EUROPEO

Roma, venerdì 24 gennaio 2014
ore 9,30-13,30

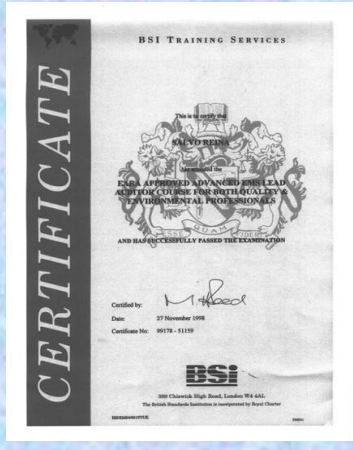
Sala conferenze del Garante per la protezione dei dati personali
Piazza di Monte Citorio n. 123/A

In collaborazione con

EY
unoLEGAL

Con il patrocinio di

FEDERPRIVACY



BSI TRAINING SERVICES

CERTIFICATE

This is to certify that

SALVO REINA

successfully attended the

EXIN APPROVED ADVANCED EMS LEAD AUDITOR COURSE FOR BOTH QUALITY & ENVIRONMENTAL PROFESSIONALS

AND HAS SUCCESSFULLY PASSED THE EXAMINATION

Certified by:
Date: 27 November 1998
Certificate No: 99178 - 51159

BSI

389 Chiswick High Road, London W4 4AL
The British Standards Institution is incorporated by Royal Charter

ZERTIFIKAT ◆ CERTIFICATE ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATO

n° CDP_041

Con il presente si certifica che

REINA SALVATORE
C.F. RNESVT60A10C342J

ha positivamente superato l'iter di certificazione in accordo allo schema CDP

Consulente della Privacy e Privacy Officer

Il sistema di gestione della certificazione delle professioni è sviluppato da TÜV Italia in conformità alla norma ISO/IEC 17024:2003 e regolamenti tecnici collegati

Per l'Organismo di Certificazione
TÜV Italia S.r.l.

Luca Boniardi
Responsabile Qualità e Accreditamenti

Data Prima Emissione: 2012-07-27
Data Emissione: 2012-07-27
Data Scadenza: 2015-07-26

Le validità del presente certificato è subordinata a sorveglianza periodica e 12 mesi

TÜV Italia • Gruppo TÜV SÜD • Via Carducci 125, Pal. 23 • 20099 Sesto San Giovanni (MI) • Italia • www.tuv.it

bsi.

Certificate

This is to certify that

Salvo Reina

has attended the course

Cloud Computing Security Training Course: Auditing Cloud Security for CSA STAR Certification

For and on Behalf of BSI

Luigi Gruosso

Date: 29/05/2014 Certificate Number ENR-0013186

...making excellence a habit.

Il Corriere della Privacy
il primo giornale sulla protezione dei dati personali

ATTESTATO DI MASTER

CONSULENTE DELLA PRIVACY
E PRIVACY OFFICER
3ª EDIZIONE

rilasciato a

Salvo
Reina

per aver frequentato il corso di complessive 40 ore "Master di specializzazione per Consulente della Privacy e Privacy Officer", conseguendo esito positivo a tutte le verifiche di apprendimento previste dal percorso formativo al termine di ogni singolo modulo. Il rilascio del presente attestato costituisce evidenza oggettiva della soddisfazione del requisito della formazione specifica richiesto dallo schema di certificazione (CDP/TÜV) della figura professionale di Consulente della Privacy e Privacy Officer.

IL CORRIERE DELLA PRIVACY

Sede: Reggio Emilia c/o Università degli Studi di Modena e Reggio Emilia
Docenti: Monica Perego, Luca Bolognini, Paolo Balboni
Durata: 40 ore
Periodo di svolgimento: Anno 2012
Reg. Formazione: CDP/2012 RF. 00058

"MASTER DI SPECIALIZZAZIONE PER CONSULENTE DELLA PRIVACY E PRIVACY OFFICER"

FEDERPRIVACY

ASSOCIAZIONE PROFESSIONALE AI SENSI DELLA LEGGE 4/2013 ISCRITTA PRESSO IL
Ministero dello Sviluppo Economico

ATTESTATO DI QUALITA'

Rilasciato ai sensi dell'art.7 della Legge 4/2013

Salvo Reina

Data Protection Officer

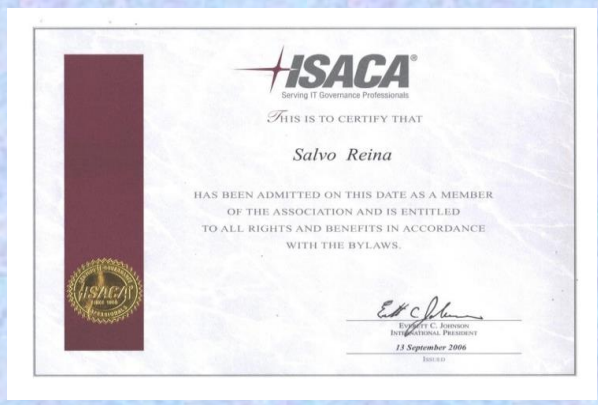
Codice Tessera:
AD100705

Codice QR per verifica validità:

Il presente attestato è rilasciato al socio promotore che, ai sensi degli artt. 4,7,8 della Legge 4/2013, alla data di emissione risulti rispettare gli standard qualitativi di Federprivacy secondo i dettagli riportati sul retro dello stesso

Firenze, 6 aprile 2016

FEDERPRIVACY
Il Presidente



ISACA
Serving IT Governance Professionals

THIS IS TO CERTIFY THAT

Salvo Reina

HAS BEEN ADMITTED ON THIS DATE AS A MEMBER OF THE ASSOCIATION AND IS ENTITLED TO ALL RIGHTS AND BENEFITS IN ACCORDANCE WITH THE BYLAWS.

Everett C. Johnson
International President

13 September 2006
Issued

CERTIFICATO

N° Registro CDP 041

Titolare: REINA SALVATORE
Codice Fiscale: RNESVT60A10C342J
Schema: Consulente della Privacy e Privacy Officer

Data Prima Emissione: 27/07/2012
Data Emissione: 27/07/2012
Data Scadenza: 26/07/2015

TÜV SÜD
Italia

Luca Boniardi
Direttore TUV Examination Institute

La validità del presente certificato è subordinato a sorveglianza periodica a 12 mesi

TUV Italia Srl - Gruppo TUV SUD - Via Carducci 125 - 20099 Sesto S G (MI) - www.tuv.it

Certificate of Training

This is to certify that:

Salvo Reina

has successfully completed the ISMS Auditor/Lead Auditor course (ISO 27001:2005)

delivered by BSI Management Systems

Date: 22/05/06 - 26/05/06
Certificate No: 26864/80890

For and on behalf of BSI:

Head of Training, BSI Management Systems (UK)

Course number A17287 certified by IRCA

THIS CERTIFICATE IS VALID FOR THREE YEARS FROM THE DATE OF THE LAST DAY OF THE COURSE FOR THE PURPOSE OF REGISTERING AS AN AUDITOR WITH IRCA

This certificate remains the property of BSI and is bound by the conditions of contract.

BSI Management Systems

CYBER CRIME CONFERENCE

ATTESTATO DI PARTECIPAZIONE

Signor *Salvo Reina*

ha partecipato al
Cyber Crime Conference
Le nuove minacce cibernetiche

27-28 Marzo 2013
Crowne Plaza Convention Centre - Roma

Roma, 27-28 Marzo 2013

TecnoEdittrice

ATTESTATO

CSQA FORMAZIONE

SALVO REINA

ha partecipato al corso

La nuova ISO/IEC 27001:2013.
Corso di aggiornamento per auditor

Tenutosi a ROMA in data 20 febbraio 2014
Durata: 8 ore

3 marzo 2014 Attestato n. 11

Dr. Pietro Bonato
Direttore Generale

La partecipazione alla presente Giornata sarà ritenuta valida ai fini dell'aggiornamento professionale richiesto per il rinnovo delle certificazioni e o qualificazioni rilasciate da AICQ SICEV/SICEP

CSQA Certificazioni Srl THIENE (VI) 36016 Via S. Gaetano, 74 - Tel. +39 0445 313070 - Fax +39 0445 313070 - csqa@csqa.it

csqa@csqa.it - www.csqa.it

ICT Security FORUM

ATTESTATO

Signor *Salvo Reina*

XII Forum ICT Security: Sicurezza Informatica

17-18 Ottobre 2012
Crowne Plaza Convention Centre - Roma

Roma, 17-18 Ottobre 2012

TecnoEdittrice

ISSA®

Information Systems Security Association

The Global Voice of Information Security

ISSA Inc., 9220 SW Barbur Blvd #119-333, Portland, OR 97219
USA: (866) 349-5818, International: +1 (206) 388-4584

Salvo Reina

2007-02-28 - 2009-02-27

Corporate Organizational Member, Number 3117752

ATTESTATO DI PARTECIPAZIONE

SALVO REINA

ha partecipato il giorno 6 luglio 2016 dalle ore 14.30 alle ore 17.30 al seminario

IL CYBERSECURITY FRAMEWORK E IL CAMMINO DI ADEGUAMENTO AL NUOVO REGOLAMENTO EU SULLA PRIVACY

Si attesta l'attribuzione di:
3 CPE di cui:

2 specifici per CCSA
2 specifici per CRMA

Associazione Italiana Internal Auditors

Profilo professionale

Excursus accademico / professionale

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

Certificazioni

Accreditamenti e affiliazioni

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

Salvo Reina

Expertise & skills

§

- Scientific e technological Ghost-writer
- Lead Auditor – ICT Governance, CPP
- Lead Analyst – IT Security, Risk Mngmt, OHSAS
- Integrator & Advisor on 231, Dlg191/07, Dlg81/08
- Certified Data Protection Officer, CDA/RPD, Regulatory Consultant
- Privacy & Safety Advisor & ICT - Blogger

tiro al piattello !