Sicurezza informatica dei Medical Device e Privacy *un matrimonio impossibile?*

Graziano de' Petris
Data Protection Officer Sanità
Vicepresidente APIHM
rpd@asuits.sanita.vfg.it

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

https://youtu.be/_mkRAArj-x0

impactscool MAGAZINE

Come i Big Data hanno cambiato il marketing

22 novembre 2019 | Scritto da Alberto Larato SISSA Trieste

Ogni giorno generiamo circa 3 quintilioni di byte, un numero enorme di dati che hanno il potere di rivoluzionare

I vostri dati vengono usati solo in ambito di marketing oppure anche di politica o sensibilizzazione su temi sociali…

Per quanto riguarda Weborama solo marketing, se mi chiedi una visione di mercato è noto che possono venire utilizzati anche in ambiti altri, politica sociali o quant'altro. In realtà dipende dalla connotazione che vuoi dare alle cose, alla fine in questo caso più che di politica parliamo di marketing politico. Nel nostro caso non è ancora successo, non escluso che possa succedere, anche se siamo con le antenne ben tese perché è molto rischioso, non credo che ci addentreremo in quel campo.

mondo, in Italia circa 50 milioni. Come vengono gestiti questi dati e qual è il loro valore?

In realtà la metafora del nuovo petrolio è significativa fino a un certo punto: del petrolio in sé ce ne facciamo poco, anzi rischia di prendere fuoco e creare disastri ambientali se non sono in grado di gestirlo e raffinarlo a dovere. È quello che ci facciamo con questo petrolio che è importante: ovvero far funzionare le automobili. Per i dati è esattamente la stessa cosa, il punto è come metterli insieme per fare previsioni più accurate possibili e quindi essere in grado di gestire il futuro e affrontarlo nel migliore dei modi possibili.

Fino a pochi anni fa, le persone che si occupavano di marketing lavoravano su Excel, con dati ottenuti tramite ricerche di mercato fatte a campione, in cui si dava per scontato che fossero rappresentative. Adesso con i big data arriviamo ad un approccio censuario, riusciamo ad avere una visione, un polso del mercato e un profilo dei consumatori che sono molto più affidabili e vicini alla realtà.

Per analizzare i dati voi sfruttate un'IA semantica, come funziona?

AREA SCIENCE PARK

Il Messaggero

Dir. Resp.:Virman Cusenza

Sezione:INNOVAZIONE TECNOLOGICA E IM... Tiratura: 130.946 Diffusione: 102.704 Lettori: 1.031.000

Rassegna del: 13/11/19
Edizione del:13/11/19
Estratto da pag.:25
Foglio:1/2

Project Nightingale

Una "talpa" rivela al Guardian che il colosso del web negli Stati Uniti avrebbe utilizzato illecitamente le informazioni sanitarie degli ospedali per sviluppare un software dotato di intelligenza artificiale

Scandalo Google: «Raccolti i dati di milioni di pazienti»

IL CASO

N[illegible] dei dati personali nel [illegible] della tecnologia. Una "talpa" ha rivelato al *Guardian* che Google è impegnata nella raccolta di dati medici personali di circa 50 milioni di pazienti in 21 Stati Usa - a insaputa loro e dei medici - da Ascension, una catena cattolica di 2600 ospedali, studi medici e altre strutture che ne fa il secondo operatore sanitario privato del Paese.

La "talpa" che ha parlato con il giornale britannico è uno dei circa 300 dipendenti che lavorano all'iniziativa, denominata Project Nightingale.

LA COMPETIZIONE

Si tratta del più grande sforzo di un gigante della Silicon Valley di mettere piede nell'industria sanitaria attraverso la gestione dei dati medici dei pazienti. Ci stanno provando anche Ama[illegible] [illegible] piattaforma di Mark Zuckerberg. [illegible] *whistle-blower* ha postato [illegible] piattaforma social *Daily Motion*, con centinaia di immagini di documenti confidenziali, anche sulle preoccupazioni espressi da dirigenti di Ascension.

Il trasferimento di dati comprende generalità, data di nascita, storia medica con analisi, diagnosi e ricoveri dei pazienti: 10 milioni finora, ma entro marzo saranno 50 o più milioni. «La maggioranza degli americani sarebbe a disagio se sapesse che i suoi dati sono stati trasferiti in modo aleatorio a Google senza adeguata salvaguardia e sicurezza», ha spiegato l'informatore, dicendosi preoccupato che la società possa vendere i dati a parti terze, usarli per pubblicità mirate o per predire i quadri patologici dei pazienti tramite le [illegible] compresa la *Health Insurance Portability and Accountability Act* [illegible] del 1996, [illegible] [illegible] di privacy, la Hipaa [illegible] in generale agli ospedali di condividere i dati con partner commerciali senza informare i pazienti ma solo se le informazioni sono usate «per aiutare l'operatore a realizzare le sue funzioni sanitarie». La talpa ritiene che vi possano essere violazioni.

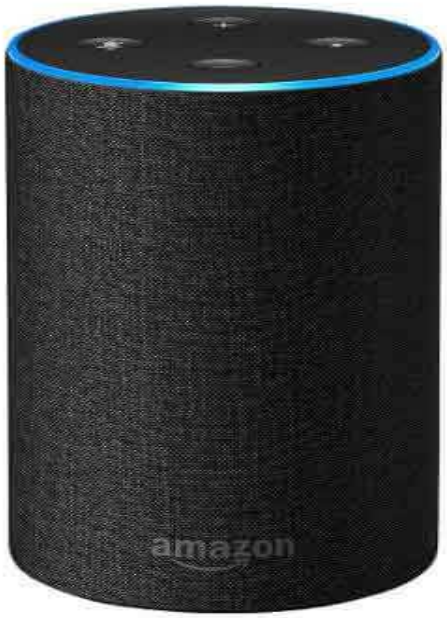
LA REPLICA

Google cloud, dal canto suo, ha dichiarato che l'obiettivo «alla fine è migliorare i risultati, ridurre i costi e salvare vite». Ma non è la prima volta che la compagnia di Mountain View scivola nei suoi sforzi di diventare il player dominante in questo settore: nel 2017 il trasferimento di 1,6 milioni di dati di pazienti del Royal Free Hospital di Londra a [illegible]

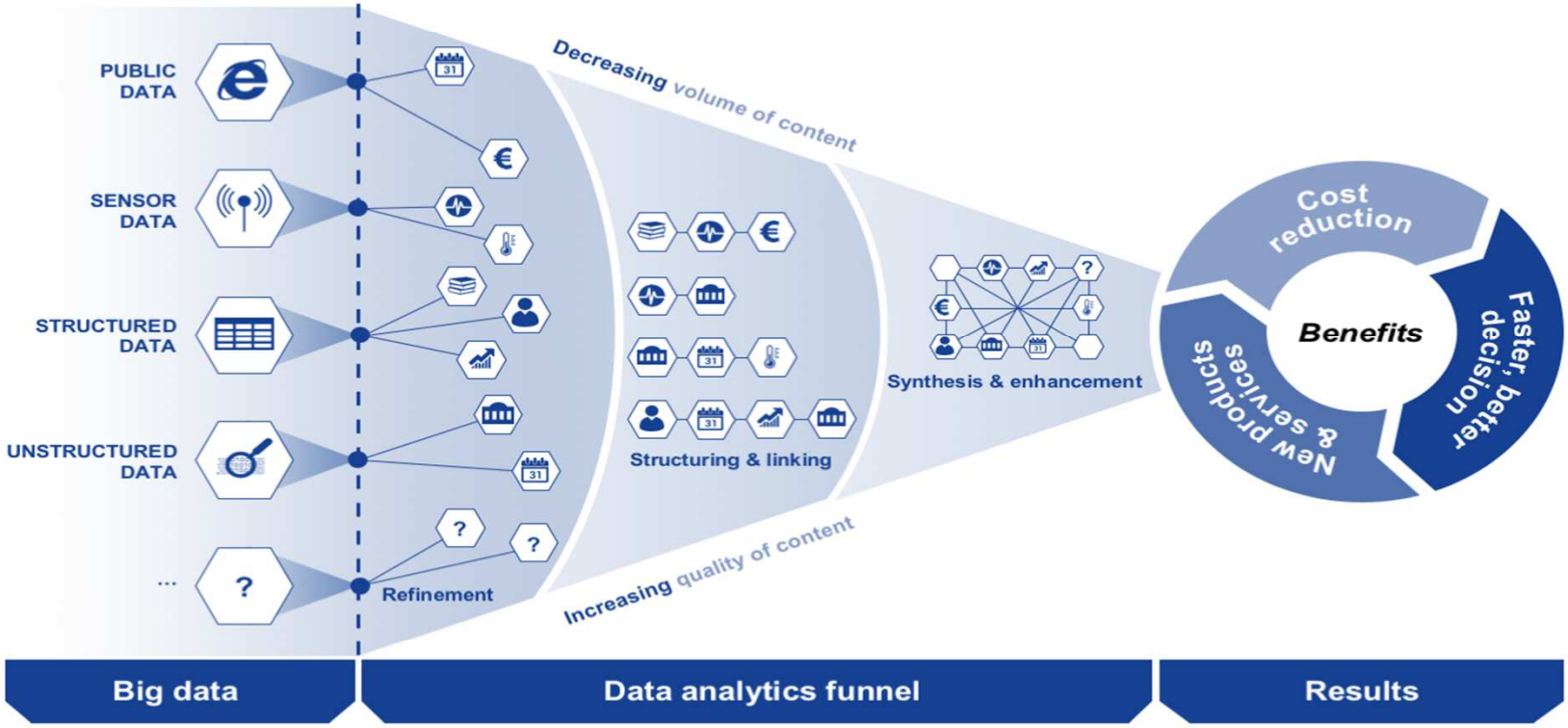
Internet of Things

Altoparlanti intelligenti

o intellighiotti?



come vengono lavorati i dati personali



Il mondo dell'impresa si è mosso subito

la PA non ha né le risorse né le competenze

l'economia dei big data

Source: Mario Morales, IDC

noi siamo i nostri dati

Soggetto Interessato al trattamento

=

la persona cui i dati si riferiscono

le decisioni sulle persone vengono prese sempre più attraverso l'analisi dei dati

la datificazione della vita
fa aumentare esponsenzialmente
l'effetto discriminatorio

questo approccio alla tecnologia non è l'unico possibile ma è quello dominante

il potere è determinato dall'asimmetria della conoscenza

in questo scenario, vedere rispettata la propria

Dignità

vedere tutelata la possibilità di esercitare le

Libertà fondamentali

poter esercitare liberamente il

Principio di autodeterminazione

…è ancora possibile?

chi tratta i nostri dati dovrebbe garantire un atteggiamento responsabile

CAPO II

LIBERTÀ

...una storia che parte da lontano...

Articolo 6

Diritto alla libertà e alla sicurezza

Ogni individuo ha diritto alla libertà e alla sicurezza.

Articolo 7

Rispetto della vita privata e della vita familiare

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Articolo 8

Protezione dei dati di carattere personale

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.


LA TOMBOLA DELLA RISATA!

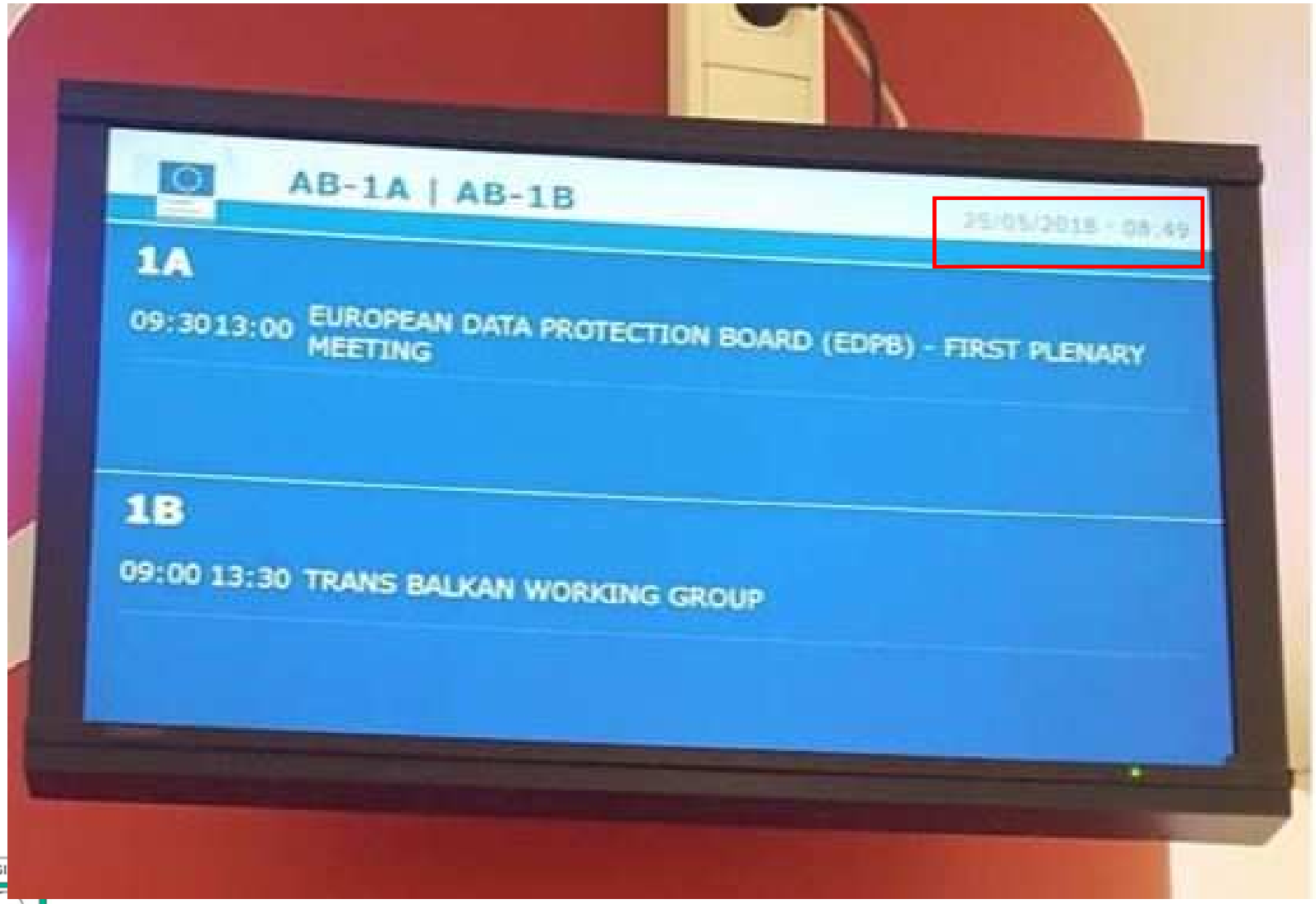
ecco perché
c'era la necessità urgente
di una nuova norma di tutela
dinamica
che si adatti ai
continui cambiamenti

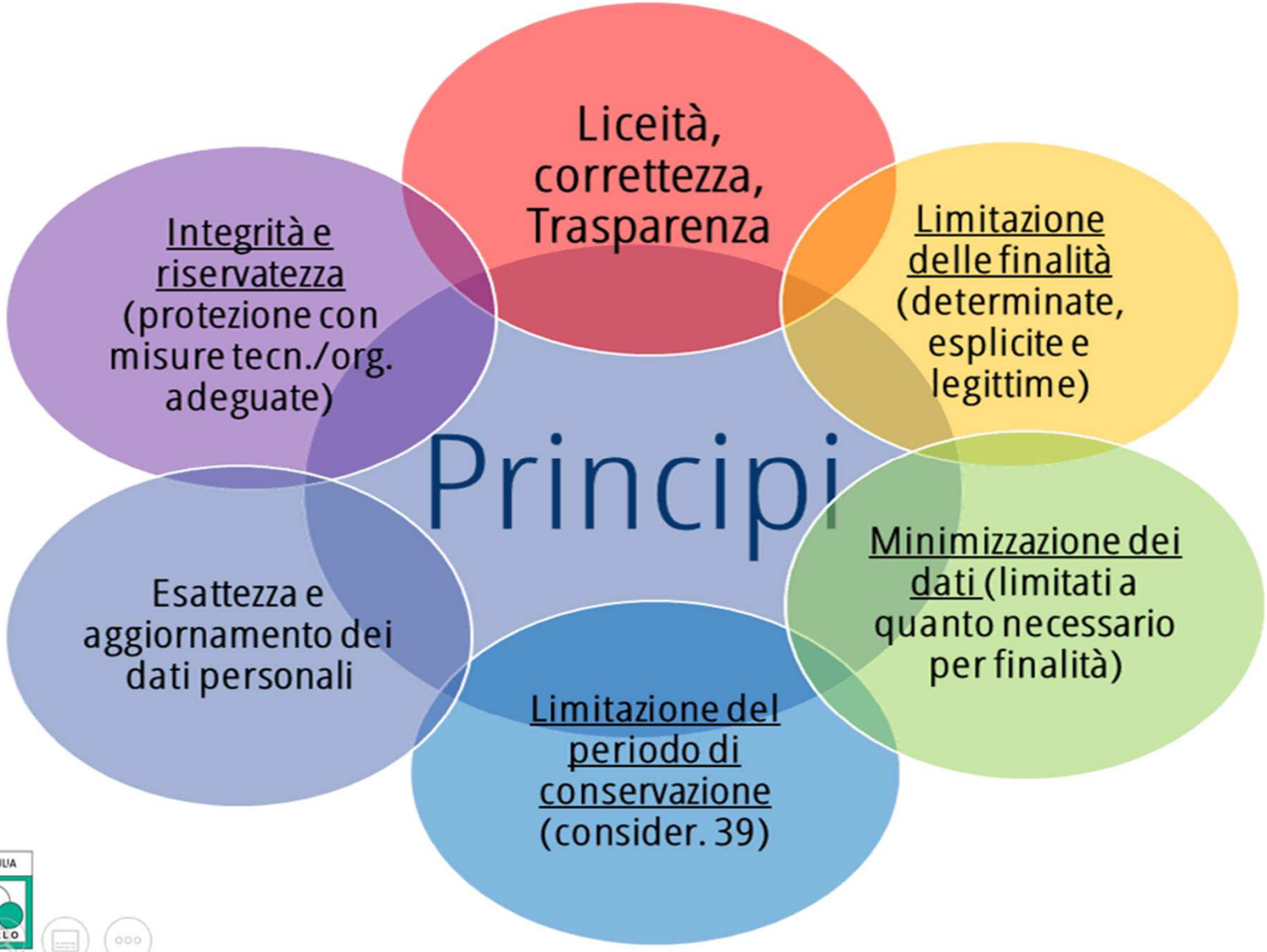

GDPR
General Data Protection
Regulation

Il dettaglio giuridico che mancava si trova ora nell'art. 5: il trattamento deve essere "**lecito, corretto e sicuro**"

Il Regolamento obbliga ad un "*trattamento corretto*"
perché ora il rapporto è tra il titolare e l'intera collettività, non solo l'interessato
violando le regole posso fare un danno a tutta la Società

*oggi tutti siamo potenziali **soggetti interessati** di un trattamento*
e sarà sempre più così, in modi che ora non possiamo nemmeno immaginare


AB-1A | AB-1B
25/01/2018 - 08:49
1A
09:30 13:00 EUROPEAN DATA PROTECTION BOARD (EDPB) - FIRST PLENARY MEETING
1B
09:00 13:30 TRANS BALKAN WORKING GROUP


Liceità, correttezza, Trasparenza
Integrità e riservatezza (protezione con misure tecn./org. adeguate)
Limitazione delle finalità (determinate, esplicite e legittime)
Principi
Esattezza e aggiornamento dei dati personali
Minimizzazione dei dati (limitati a quanto necessario per finalità)
Limitazione del periodo di conservazione (consider. 39)

Articolo 6
Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre **almeno una** delle seguenti condizioni:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

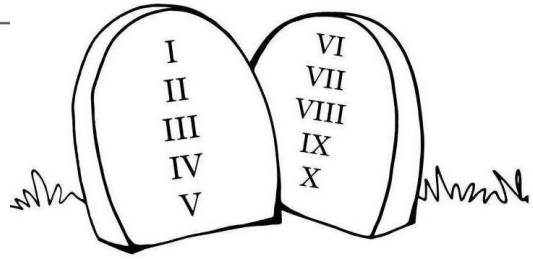
c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli **interessi vitali** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di **interesse pubblico** o connesso all'esercizio di **pubblici poteri** di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **legittimo interesse** del titolare del trattamento o di terzi, *a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali* dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.



Caro Titolare del trattamento,
devi **definire e strutturare** un modello di gestione dei dati
GDPR-conforme e ne devi garantire il rispetto
attraverso la corretta applicazione dei principi del Regolamento
e devi metterti in grado di poterne dimostrare la conformità
all'interno della tua organizzazione
Puoi farti aiutare dal DPO

Misure di sicurezza GDPR:
principio di Accountability, art. 5, c2 e art. 24
misure tecniche e organizzative adeguate art. 25 e 32

GDPR Art. 25, comma 2: **il Titolare o il Responsabile devono mettere in atto le misure organizzative e tecniche affinché, *by default*, vengano raccolti solo i dati strettamente necessari**

Minimizzare la quantità di dati raccolti, privilegiando quelli che rendono meno immediata l'identificazione dell'interessato

Minimizzare l'utilizzo e l'estensione del trattamento, in base alle finalità specifiche, evitando conservazioni non necessarie dei dati

Minimizzare la durata del periodo di conservazione

Minimizzare l'accesso ai dati personali, sia dal punto di vista di dove questi sono conservati, sia rispetto ai diritti di accesso in capo a terzi.

OBBLIGHI

ISTRUZIONE

Chiunque abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento.

Istruzione – anche non formale, significa:

*capacità di **saper fare** quello che si deve fare*

*capacità di **non fare** quello che non si sa fare*

ora la legge non ci dice più

che cosa dobbiamo fare

(*adempimenti formali*)

ci dice soltanto che in qualsiasi momento dobbiamo poter dimostrare di

essere a posto

(*adempimenti sostanziali*)

PER RISPONDERE ALLE SFIDE ED AGLI OBBLIGHI

DERIVANTI DA CAD, AgID e RGPD

È NECESSARIA UNA ORGANIZZAZIONE TRASVERSALE

SNELLA ED EFFICACE

SINERGICA SUI 3 ARGOMENTI

CHE GARANTISCA RISPONDENZA UNIFORME AGLI OBBLIGHI

SENZA SOVRAPPOSIZIONI

QUESTA ORGANIZZAZIONE

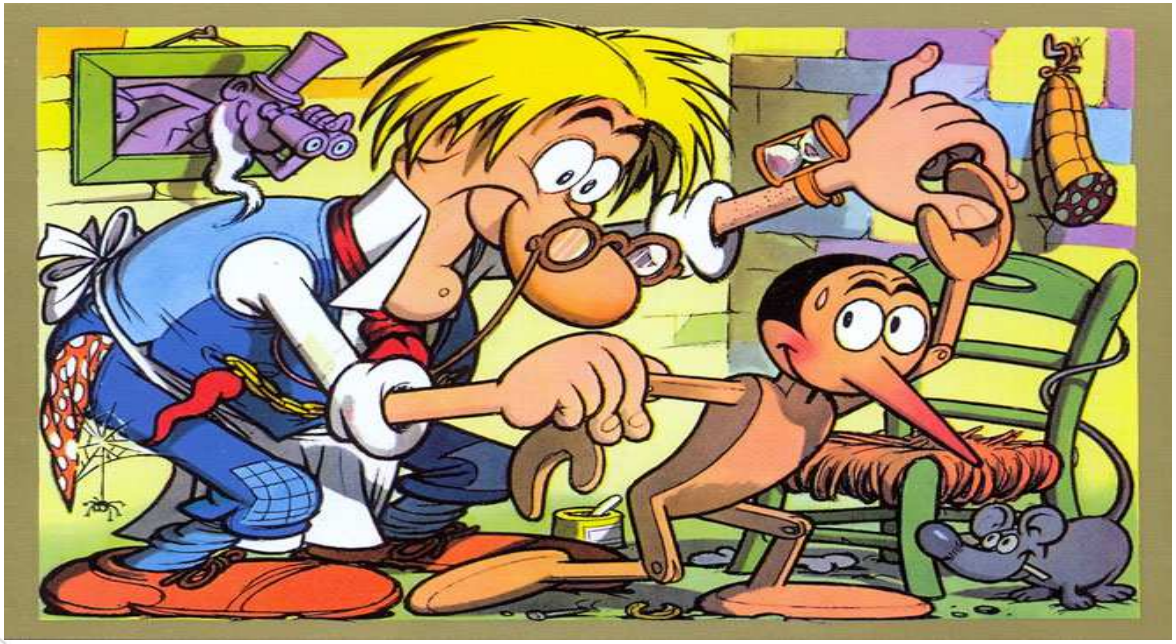
NON PUO' ESSERE REALIZZATA A COSTO ZERO

UE 679/2016

art. 23-25 (e Capo IV in generale):

data protection by default and by design

è richiesto al titolare di essere proattivo!



Dal dato come informazione al dato come valore

APPROCCIO BASATO SUL RISCHIO E MISURE DI RESPONSABILIZZAZIONE

E' stato necessario introdurre nuovi obblighi

Privacy by design

quando voglio mettere in atto un trattamento devo pensare già mentre lo progetto

a come proteggere i dati personali

Privacy by default

devo predisporre misure tecnologiche, ma anche organizzative,

per ridurre al minimo i rischi che il trattamento può far correre ai dati

Data Protection Impact Assessment

Introduzione del

Data Protection Officer

Accountability

Prima regola del GDPR:

PROTEGGI IL DATO
IN TUTTO IL SUO CICLO DI VITA

Ma… in pratica?

in quale delle tre fasi si trovano i dati
(*solida, liquida, gassosa?)*

1. a riposo – in conservazione
2. in movimento – in trasmissione
3. in uso – in trattamento

il dato va protetto in modo omogeneo
mentre si muove nello spazio e nel tempo
per tutto il suo ciclo di vita

proviamo a confrontare le prescrizioni di legge
con le relative attività informatiche

LEGGE

Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

§1 dice: ... sia al momento di determinare i mezzi del trattamento (**software di «qualità»**) sia all'atto del trattamento stesso (**procedure online o batch**) il titolare del trattamento 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 (**storicizzazione - vedi considerando 156)** ..

§2 dice: Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità (**profili**) del trattamento ....

*§3 dice: **Un meccanismo di certificazione** approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo*

Art. 32 - Sicurezza del trattamento (uso di sistemi software + hardware)

***§1** dice: Tenendo conto dello stato dell'arte .... come anche del rischio (**art. 35 - PIA**) di varia probabilità e gravità .... il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (**misure di attenuazione del danno e riduzione della probabilità**), ... se del caso...*

a) la pseudonimizzazione e la cifratura dei dati personale

*b) la capacità di assicurare su base permanente la riservatezza (**controllo degli accessi 1° e 2° liv....**), l'integrità (**alterazione**), la disponibilità (**Backup e Restore; sistemi di continuità**) e la resilienza dei sistemi (**SW + HW → BC o DR**) e dei servizi di trattamento (**BC e DR**)*

*c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (**BC e DR**)*

*d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (**SW + HW**) e organizzative (**ciclo di vita del SW -sviluppo e esercizio-: SW, processi e ruoli**) al fine di garantire la sicurezza del trattamento*

*§2 dice: ... si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione (**loss**), dalla perdita (**loss**), dalla modifica (**loss**), dalla divulgazione (**leak; estrusione**) non autorizzata o dall'accesso (**leak; intrusione**), in modo accidentale o illegale, a dati personali trasmessi (**in movimento**), conservati (**a riposo**) o comunque trattati (**in uso**)* → ***ATTENZIONE!*** → ***Introduzione dei processi per la gestione del DLP***

TECNOLOGIA

1. Mezzi del trattamento (**software di «qualità»**) - procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (software) e organizzative sia nel ciclo di vita del software in ambiente di Sviluppo sia in Esercizio al fine di garantire la sicurezza del trattamento:
   a. la riduzione o l'annullamento della vulnerabilità ***(es.: istruzioni del sorgente)*** con strumenti di:
      - *Change Management Ciclo di vita del sw*
        - analisi STATICA (**STATIC APPLICATION SECURITY TESTING**)
        - test DINAMICO (**DYNAMIC APPLICATION SECURITY TESTING**)
        - test PT (**PENETRATION TESTING**)
        - test INTERATTIVO (**INTERACTIVE APPLICATION SECURITY TESTING**)
      - *Sicurezza perimetrale*
        - protezione RUNTIME (**RUNTIME APPLICATION SELF PROTECTION**)
        - protezione del WEB (**WEB APPLICATION FIREWALL**)

   b. controllo accessi e profili utenze con strumenti di:
      - *Solo dati necessari e controllo anomalie o errori*
        - identificazione e di controllo degli accessi
        - raccolta e di classificazione dei dati (impostazione predefinita)
        - analisi dei log e di monitoraggio
2. *Protezione dei dati* Strumenti per la: Pseudonimizzazione, Minimizzazione, Cifratura
3. Disponibilità del dato: procedure e programmi di **Backup e Restore;** strumenti di **analisi dei log** e di **monitoraggio**
4. Resilienza dei sistemi SW, HD e servizi di trattamento: procedure e programmi di **Backup e Restore, strumenti di analisi dei log e di monitoraggio**
5. Incidente fisico o tecnico: procedure tecniche ed organizzative per la gestione della **Business Continuity** ed il **Disaster Recovery**
6. Distruzione (**loss**), Perdita (**loss**), Modifica (**loss**), Divulgazione (**leak; estrusione**) non autorizzata o Accesso (**leak; intrusione**), di dati personali
7. Trasmessi (**in movimento**), Conservati (**a riposo**), Trattati (**in uso**)

Le norme sono convergenti!

- UE - Regolamento DM 2017/745 (26 maggio2020)
- UE - Regolamento privacy 2016/679 (25 maggio 2018) e IT - Dlgs 101/2018
- AGID misure minime sicurezza PA (31 dicembre 2017)
- DLgs 81/2008 sicurezza sul lavoro

E SAPPIAMO ANCHE COME APPLICARLE

- ISO – 31000 Risk Management – *i principi*
- ISO – 80001-1 Risk Management – *delle reti IT medicali*
- CEI - 62-237-1 *Gestione del software nel contesto sanitario*
- CIS - Critical Security Controls for Effective Cyber Defense - *Version 7.0* (SANS Institute)

Il fatto è che bisogna STUDIARE *e fare* FORMAZIONE…

l'attività ispettiva del Garante ad una anno dal GDPR
evidenzia ancora una disattenzione costante alle norme privacy

bisogna passare dalla forma (spesso informe)

alla sostanza

sono emersi aspetti molto critici della maglia di protezione attorno ai dati
che troppo spesso è solo teorica

il GDPR focalizza le misure per la sicurezza e impone l'analisi dei rischi
ma questo era richiesto anche prima dalle best practice

ora **accountability** significa la responsabilizzazione **di tutti gli attori**
non solo del legale rappresentante

significa non solo che devi fare le cose e cercare di farle al meglio
in modo **efficace** ed **efficiente**
ma le devi anche **documentare**
perché in caso di ispezione devi dimostrare di avere fatto **effettivamente**
gli interventi previsti
l'obbligatorietà della segnalazione di un Data Breach è un fatto molto delicato e
impegnativo che può provocare gravi conseguenze


LA LEGGE
È UGUALE
PER TUTTI
QUELLI CHE
DICO IO

in pratica
bisogna *pensare* al rispetto
delle regole di tutela integrate
fin da quando si *pensa*
di acquisire un'apparecchiatura,
una tecnologia, un servizio, …

anche perché le sanzioni amministrative sono personali

(L. n. 689/1981 e ss.mm.ii.)

chi ha mancato all'obbligo di garantire il rispetto della normativa in materia di riservatezza

risponderà personalmente della violazione commessa

Agenzia Europea per la sicurezza delle reti e delle informazioni

Recommendations on shaping technology according to GDPR provisions

Exploring the notion of data protection by default

DECEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

le impostazioni predefinite sono determinanti per la sicurezza e la protezione dei dati, già dal primo utilizzo di un sistema o di un servizio

Ma sono determinanti anche per gli utilizzi successivi nel lungo periodo

GDPR Art. 25, comma 2

"Il Titolare o il Responsabile devono mettere in atto misure organizzative e tecniche affinché, by default, vengano raccolti solo i dati strettamente necessari"

La pseudonimizzazione non è una misura obbligatoria, ma può essere adottata al termine di un delicato processo di bilanciamento fra i costi, la natura, l'oggetto, il contesto e le finalità del trattamento, nonché dei rischi che questo comporta.

è sempre più difficile proteggere i dati affidati dalle vulnerabilità introdotte dalle terze parti

*non a caso la **protection by default***

è **la principale** delle Raccomandazione di ENISA…

Tre azioni *suggerite* per migliorare l'adeguamento:

- **Governance:** aumentare la collaborazione con altri titolari, responsabili di governo e autorità di regolamentazione per definire un modello comune omogeneo di prevenzione dei cyber-attacchi

- **Business Architecture:** connettere e proteggere i titolari tramite un modello basato sulla fiducia digitale

- **Tecnologia:** adottare nuove tecnologie, ma gestire la sicurezza dell'IoT, assicurandosi che la sicurezza dei software e le funzioni di aggiornamento siano integrate nei dispositivi mobili e IoT sin dalla loro progettazione

In particolare, gli interventi richiederebbero:
competenze nel settore delle tecnologie informatiche;
uso di prodotti per la **protezione e classificazione dei dati**;
verifica statica e dinamica delle vulnerabilità del software;
verifica delle **compliance** del software libero;
revisione delle procedure organizzative.

interventi efficaci richiederebbero:

- **competenze nel settore delle tecnologie informatiche;**
- **uso di prodotti per la protezione e classificazione dei dati;**
- **verifica statica e dinamica delle vulnerabilità del software;**
- **verifica delle *compliance* del software libero;**
- **revisione continua delle procedure organizzative.**

La Sanità è l'ambiente dove le problematiche applicative del GDPR sono le più complesse

Il sistema di gestione potrebbe essere

Paziente-centrico;

Dato-centrico;

Sistema-centrico;

…

un sistema gestionale a norma e sostenibile
non può che essere

Diritto-d'accesso-ai-dati-centrico

- *Profili d'accesso ai dati corretti e adeguati*
- *Distribuzione e controllo delle responsabilità*

Innanzitutto è indispensabile conoscere come avviene ogni trattamento di dati

…e prima ancora decidere cosa si intende per trattamento…

Basta con gli adempimenti formali!

ma ricordiamoci che anche protocolli e procedure hanno bisogno di manutenzione

LE FIGURE E I RUOLI

NELLA GESTIONE DELLA PRIVACY DOPO IL GDPR

REGIONE AUTONOMA FRIULI VENEZIA GIULIA
ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO
Burlo Garofolo di Trieste
BURLO

Gerarchia della Privacy

dopo il Regolamento (UE) 2016/679 e l'adeguamento del «Codice Privacy» con il Dlgs 101/2018

RPD
(DPO)

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE

Gruppo di lavoro multidisciplinare

Legale Rappresentante

Titolare

Dirigenti Subordinati

DIR - TD

AUTORIZZATI FORMATI

AMMINISTRATORI DI SISTEMA FORMATI

soggetti Interessati al trattamento

Le figure

Privacy Specialist – livello operativo

attività operativa, figura tecnica, esperienza informatica o di tecniche delle comunicazioni, **solide competenze ICT**

Privacy Manager – livello gestionale

Attività di coordinamento dei trattamenti e della loro gestione, **esperienza di management dei processi**

Data Protection Officer - supervisione

Figura indipendente di garanzia, funzioni di controllo, di indirizzo, di supporto alle strutture operative per superare le difficolta nell'applicazione del GDPR, **competenze ed esperienze multiprofessionali**

Norma UNI 11679:2017

IL DATA PROTECTION OFFICER (RESPONSABILE DELLA PROTEZIONE DEI DATI)

Art. 37, 38 e 39 Reg. UE 679/2016

Nomina obbligatoria nelle ipotesi di cui all'art. 37 comma 1

il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali)

Fra i compiti del RPD rientrano

"la sensibilizzazione e la formazione del personale" e la sorveglianza

sullo svolgimento della valutazione di impatto

I requisiti del DPO

- Conoscenza **accurata** della normativa Europea e nazionale
- Esperienza **pregressa** di gestione della Privacy e della sicurezza informatica
- Competenze **tecniche** e conoscenza della tecnologia ICT, benefici e pericoli
- **Indipendenza**
- Capacità **manageriali**
- **Autorevolezza**
- Competenze **relazionali**
- …

I compiti del DPO

- Informare e consigliare
- Verificare e monitorare
- Fornire pareri su richiesta
- Fungere da punto di contatto per: Garante, Interessati, altri Enti, Fornitori,…

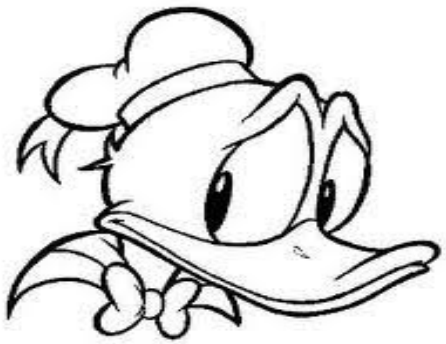
…e gli elementi ancora da chiarire:

Formazione?

Certificazioni?

Contratto?

Inquadramento?



il DPO ha bisogno di informazioni!

DPO e Privacy Manager devono poter disporre di una mappa
che indichi dove sono allocati i vari ***giacimenti di dati***
quale sia la loro natura
quali siano i criteri con cui sono accessibili
quali protezioni sono in atto
quali sono le potenziali minacce di accesso indebito
e di uso inappropriato o fraudolento

l'architettura gestionale va documentata con un
Registro dei Processi e dei Dati
Propedeutica alla definizione del Registro dei Trattamenti

va eseguito l'Assessment del Rischio per ottenere la DPIA
(*Data Protection Impact Assessment*)

- per identificare le lacune del sistema di protezione in essere (anelli deboli della catena della sicurezza)
- per tracciare gli accessi inappropriati e la probabilità che possano verificarsi)
- per valutare la vulnerabilità del sistema di protezione messo in atto
- per definire il valore del rischio residuo e se sia accettabile

dal report della conservazione dei dati
- si ottiene il **registro dei trattamenti**
- si **mappano** i flussi di lavoro
- si **definisce** e si **mantiene aggiornato** un inventario dei dati

…in tutto questo c'è una sola certezza…

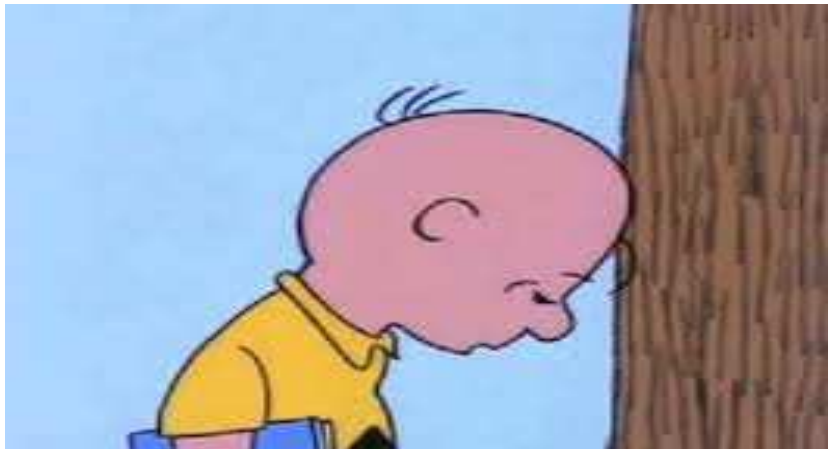
…il DPO NON è la Fata Turchina…

la valutazione del rischio è particolarmente complessa e delicata
*quando il rischio è legato ai fornitori di **software che generano dati***
*o ai **fornitori di dati***

va controllata anche la **sicurezza** dei fornitori, vanno valutati **i loro rischi**

non è facile fare una valutazione attenta degli incidenti
e delle violazioni che avvengono

la materia è complessa e incerta, soprattutto per le grandi realtà
chi fa la valutazione deve fare molta attenzione alla responsabilità che assume
gli eventuali errori sono perseguibili legalmente



il ruolo del DPO è caratterizzato da **competenze multidisciplinari**
deve interagire **strettamente** con il Privacy Manager, l'ICT Manager, e con il Titolare

ma il problema è l'effettiva protezione dei dati
il solo elemento concreto che permette di verificare
che l'approccio e la soluzione dei problemi di protezione
sono stati risolti e sono solidi e consistenti

il DPO deve **aiutare** il titolare a supervisionare ciò che viene fatto
si focalizza su quattro macro-livelli di competenze
tecniche, di **sicurezza informatica**, **legali**, **organizzative**

deve essere capace di **contestualizzare** su una certa struttura organizzativa dell'azienda o dell'ente e sulla sua cultura

*Il DPO deve essere dotato di **capacità manageriali** e **relazionali**, perché deve svolgere un'attività trasversale a tutte le articolazioni organizzative dell'Ente*

Nessuno può sapere tutto né conoscere tutto

referenti e responsabili interni devono interfacciarsi tra loro e con le terze parti perché molti trattamenti di dati personali sono terzializzati

in settori particolarmente complessi come la Sanità
bisogna conoscere anche tutte le altre normative vigenti
che vanno coordinate con quella sulla protezione dei dati personali

Il DPO in ambito sanitario svolge una funzione di alta complessità
nel sistema sanitario ci sono tantissime tipologie di trattamento
il sistema sanitario è una delle amministrazioni più complesse

perché l'attività sanitaria risponde a logiche pubbliche
anche i liberi professionisti rispondono nel loro operato
e negli atti che sottoscrivono
a particolari requisiti di valore medico legale

va rispettato non solo il GDPR, ma anche tutta quella parte del 196
modificato dal decreto legislativo 101/18 che rimane comunque vigente

chi si sia già sia certificato UNI 11697:2017 come Data Protection Officer, sappia che
la norma non comprende competenze per profili specifici in ambito sanitario
va bene come norma che può dimostrare alcune competenze acquisite
ma non differenzia un tipo di DPO dall'altro

c'è ancora tanto da fare

- in termini di stabilizzazione delle competenze
- sulle le modalità operative
- **sulla formazione delle figure privacy**

bisogna sviluppare la capacità di contestualizzare

anche se ci sono elementi simili nei vari contesti
i DPO si dovranno specializzare per tipologia di contesto

ambito sanitario, **ambito finanziario**, **ambito industriale**, **ambito dei servizi**

i DPO del sistema pubblico dovranno possedere requisiti più stringenti di quelli del privato, in particolare in Sanità
perché i dati custoditi dal Sistema Sanitario Nazionale sono un bene dei cittadini

…e le certificazioni?

Certificazione di prodotto o servizio
ISO 17065, come ad es. lo schema ISDP 10003:2015 – Criteri e regole di controllo per la Certificazione dei processi per la tutela delle persone fisiche con riguardo al trattamento dei dati personali – Reg. EU 679/2016.

Certificazione delle figure Professionali della Data Protection UNI 11697:2017 DPO, Auditor Privacy, Privacy Officer e Consulente Privacy

Certificazione del Data Protection Management System delle Aziende in conformità al Codice di Condotta DPMS 44001:2016© ed al Reg. (UE) 679/2016

Certificazione del sistema di gestione della sicurezza delle informazioni_ISO 27001:2013

*le certificazione sulla privacy possono **aiutare***
*ma **non esimono** i titolari e i responsabili del trattamento*
dall'essere passibili di sanzioni

Non si è ancora affermato un sistema di gestione della privacy ufficialmente riconosciuto
che, sulla base della struttura **HLS** (High Level Structure)
delle norme sui sistemi di gestione (ISO 9001, ISO 27001, ecc.),
consenta di gestire la protezione dei dati
con un **approccio sistemico** basato sui processi e su concetti
come il *risk based thinking* e sull'attuazione di azioni finalizzate
ad affrontare i potenziali rischi sul trattamento di dati personali

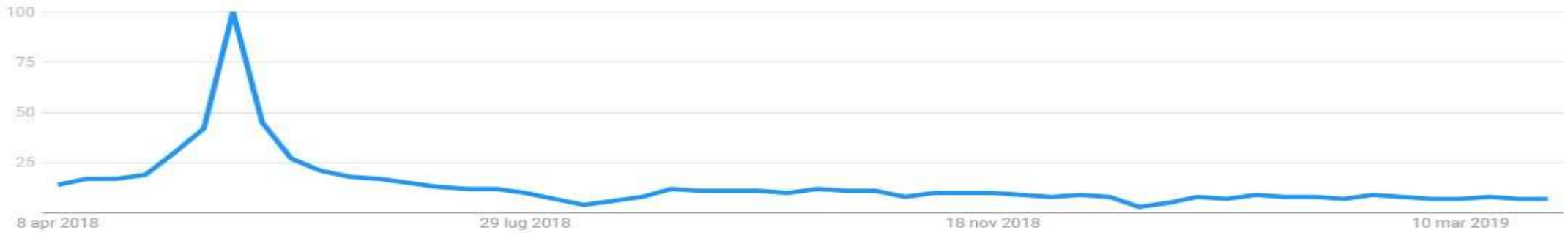
Il ruolo del Data Protection Officer (DPO o RPD)
come definito dal Regolamento
non corrisponde ancora ad una figura professionale specifica
con requisiti di competenza ben determinati
istruzione scolastica e post scolastica, conoscenze normative e tecniche, esperienza in ambito privacy, partecipazione a corsi di formazione continua,
*superamento di **esami di Stato***
mancano ancora

il DPO è quindi un ruolo
che richiede competenze differenti
a seconda della realtà in cui opera
e delle criticità sulla protezione dei dati personali
nella specifica organizzazione

questa impostazione, associata agli standard
permetterebbe di ridurre il rischio
che il titolare del trattamento e gli eventuali responsabili
incorrano in infrazioni nel trattamento di dati personali
e rischino sanzioni anche molto pesanti
e/o gravi danni di immagine

Regolamento generale sulla protezione dei dati — Italia, Ultimi 12 mesi

Interesse nel tempo



in Italia le ricerche con argomento GDPR su Google hanno avuto un picco soltanto il 25 maggio 2018

Interesse per regione

1	Friuli-Venezia Giulia
2	Veneto
3	Lombardia
4	Piemonte
5	Emilia-Romagna

Google Trends

ci sono molti anelli deboli

ma dipende tutto da noi

ricordatelo sempre!

graziano.depetris@dia.units.it


GDPR
General Data Protection
Regulation