Aspetti del Regolamento UE 2016/679

Samantha Profili

Referente Relazioni istituzionali, Centro Nazionale Sangue

Istituto Superiore di Sanità, Roma

Consultazione plenaria – Roma, 28 maggio 2018

Conflitto di interessi

Il sottoscritto, in qualità di Relatore,

dichiara che

- nell'esercizio della sua funzione e per l'evento in oggetto, **NON E'** in alcun modo portatore di interessi commerciali propri o di terzi;
- dichiara inoltre che gli eventuali rapporti avuti negli ultimi due anni con soggetti portatori di interessi commerciali **non sono tali da permettere a tali soggetti di influenzare** le sue funzioni al fine di trarne vantaggio.

CENTRO NAZIONALE SANGUE

Regolamento generale sulla protezione dei dati (GDPR)

Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

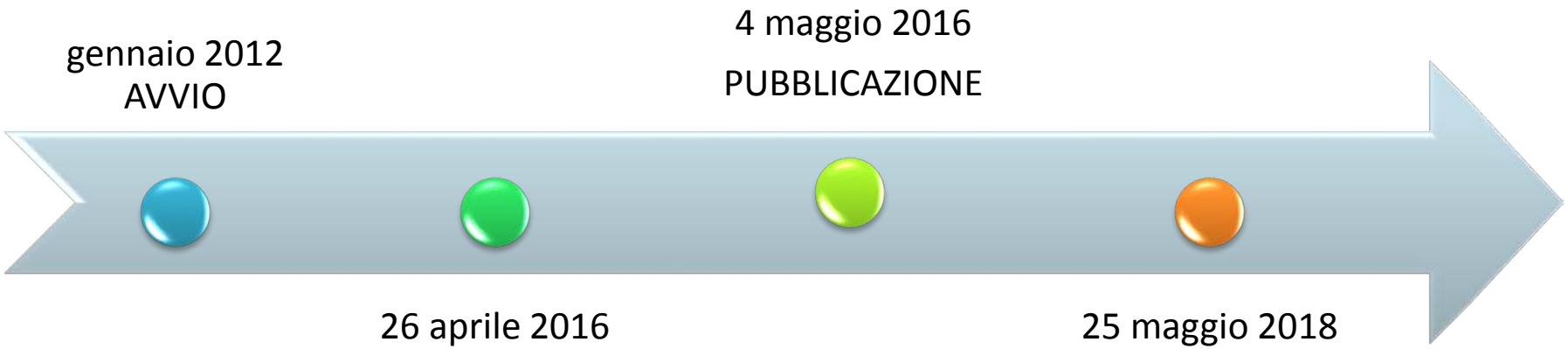
relativo alla **protezione delle persone fisiche** con riguardo al **trattamento dei dati personali**, nonché alla **libera circolazione** di tali dati e che abroga la direttiva 95/46/CE

CENTRO NAZIONALE SANGUE

Nuovo Regolamento

Perché?

- Contesto normativo uniforme in UE
- Assicurare libera circolazione dei dati
- Utilizzo tecnologie sempre più avanzate
- Tutelare i diritti dei cittadini UE anche quando il trattamento dei loro dati personali avviene fuori UE



CENTRO NAZIONALE SANGUE

Quadro normativo italiano

La Legge delega 25/10/2017 n. 163 ha previsto un **decreto legislativo** per adeguare il quadro normativo nazionale alle disposizioni del regolamento (21/3/2018 primo schema approvato) per:

- **abrogare o aggiornare** la norma incompatibile/precedente**;**
- **definire le materie** che il regolamento consente agli Stati membri di regolare (trattamenti di dati nei settori della informazione, salute, lavoro, ricerca scientifica, statistica e storica, sanzioni penali).

Ambito di applicazione del Regolamento

- Si applica al trattamento interamente o parzialmente **automatizzato** di dati personali e al trattamento non automatizzato di dati personali contenuti in un **archivio**.
- Si applica solo al trattamento di dati personali delle **persone fisiche**.
- **Non si applica** a trattamenti di dati personali da parte di una persona fisica **per attività a carattere personale o domestico**, **ma**…

Dove stiamo andando: dal Codice nazionale al Regolamento UE

- Se siamo sulla strada tracciata dal Codice siamo a buon punto.
- No compiti da assolvere ma obiettivi da garantire nel trattamento dei dati: **EFFICACIA** non BUROCRAZIA.
- Responsabilizzazione e autonomia dei soggetti titolari e/o responsabili del trattamento (**accountability**) .
- No situazioni preconfezionate ma **valutazion**i caso per caso a cominciare dai rischi nel trattamento.
- **Chiarezza e trasparenza** a vantaggio dei **diritti** degli interessati.

CENTRO NAZIONALE SANGUE

Alcune definizioni - 1

TRATTAMENTO: operazione o insieme di operazioni, con o senza ausilio di processi automatizzati, applicate a dati personali (raccolta, registrazione, organizzazione, conservazione, modifica, estrazione, consultazione, uso comunicazione, messa a disposizione, raffronto, cancellazione, distruzione)

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile (**SOGGETTO INTERESSATO**), direttamente o indirettamente (nome, numero di identificazione, identificativo on line, voce, immagine, elemento fisico, fisiologico, genetico, psichico)

Alcune definizioni - 2

DATI GENETICI: relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione

DATI BIOMETRICI: i dati ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca (immagine facciale, impronte digitali)

DATI RELATIVI ALLA SALUTE: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano lo stato di salute

DATI PARTICOLARI (ex sensibili) art. 9

Categorie particolari di dati personali

E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Tranne se …

- l'interessato ha prestato il proprio consenso esplicito al trattamento;
- il trattamento è necessario per tutelare un interesse vitale dell'interessato;
- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica (a garanzia di parametri elevati di qualità dell'assistenza sanitaria), sulla base del diritto UE e con misure specifiche di tutela (es. segreto professionale);

CENTRO NAZIONALE SANGUE

Liceità del trattamento

I fondamenti di liceità del trattamento dei dati (art. 6) coincidono, in linea di massima, con quelli previsti dal Codice. I dati devono essere/trattati:

- in modo lecito, corretto, trasparente;
- per finalità determinate, esplicite e legittime (non variazioni di finalità eccetto ai sensi dell'art. 89);
- adeguati, pertinenti e limitati (principio di MINIMIZZAZIONE);
- esatti e aggiornati, ivi compresa la cancellazione;
- conservati per un arco di tempo non superiore alle finalità (vedi art. 89);
- in modo da garantire sicurezza e integrità (da trattamenti non autorizzati o illeciti, perdita, distruzione, danni accidentali).

Consenso informato

CAMBIA	• Il titolare **DEVE** essere in grado di dimostrare il consenso ricevuto. • **NON** necessariamente "documentato per iscritto"(es. intervista telefonica registrata, moduli on line). •Per i dati "particolari" deve essere **esplicito**. •La "forma scritta" configura l'**inequivocabilità** del consenso e il suo essere "esplicito" per i dati particolari
NON CAMBIA	• **DEVE** essere, in tutti i casi, libero, specifico, informato e inequivocabile. • **NON** è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo). • **DEVE** essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" .

Il consenso raccolto precedentemente resta valido se ha tutte le caratteristiche di legge. In caso contrario, è opportuno adoperarsi per raccogliere nuovamente il consenso, se si vuole continuare a fare ricorso a tale base giuridica.

CENTRO NAZIONALE SANGUE

Informativa

CAMBIA	CONTENUTI PIU' AMPI: •**i dati di contatto del DPO**, ove esistente, •**la base giuridica del trattamento,** •**l'interesse legittimo del Titolare** se ne è la base giuridica**,** •eventuale **trasferimento in Paesi terzi** e strumenti utilizzati, •**periodo di conservazione dei dati o i criteri seguiti,** •**diritto di presentare un reclamo all'autorità di controllo** POSSIBILE RACCOLTA DATI NON PRESSO L'INTERESSATO •**tempi e modi informativa art. 14**
NON CAMBIA	•Deve essere fornita all'interessato **prima della raccolta dei dati** •Il titolare deve precisare: la propria **identità**, le **finalità del trattamento**, i **diritti** degli interessati, se esiste un **responsabile del trattamento** e la sua identità, i **destinatari** dei dati.

Informativa - 2

La richiesta di consenso deve essere **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno di modulistica.

La formula deve essere **comprensibile, semplice, chiara**.

I soggetti pubblici non devono, di regola, chiedere il consenso.

I soggetti coinvolti nel GDPR - 1

TITOLARE DEL TRATTAMENTO/CONTROLLER

La persona fisica o giuridica, pubblica o privata, che determina le finalità e i mezzi (principali) del trattamento di dati personali

RESPONSABILE DEL TRATTAMENTO/PROCESSOR

La persona fisica o giuridica, pubblica o privata, che tratta dati personali per conto del titolare del trattamento

RESPONSABILE DELLA PROTEZIONE DEI DATI / DATA PROTECTION OFFICER (DPO)

Nuova figura, nominata dal Titolare o dal Responsabile del trattamento, obbligatoria solo in alcuni casi ma sempre consigliata, punto di contatto per il Garante

I soggetti coinvolti nel GDPR - 2

PERSONA AUTORIZZATA/AUTHORISED PERSON al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile“ (≠INCARICATO) (*art. 4)*

DESTINATARIO/RECIPIENT

Persona fisica o giuridica, autorità pubblica o altro organismo che riceve comunicazioni di dati personali, che si tratti o meno di terzi. Le autorità pubbliche che ricevono dati a norma di legge non sono tali

TERZO/ THIRD PARTY

Persona fisica o giuridica, autorità pubblica o altro organismo che non sia l’interessato, il titolare, il responsabile del trattamento, persona autorizzata.

CENTRO NAZIONALE SANGUE

Il titolare del trattamento

•Mette in atto (aggiornandole) **MISURE TECNICHE E ORGANIZZATIVE** adeguate e **POLITICHE** adeguate per garantire, ed essere in grado di dimostrare, la conformità del trattamento (obbligo generale).

•La titolarità può derivare da fonte: legale, negoziale, fattuale; da inadempimento (art. 28.10).
•Si distingue per autonomia e necessarietà
• Ha obblighi specifici di:

1. informazione e comunicazione (pubblico, interessato, violazioni)
2. sicurezza,
3. designazione (responsabile del trattamento, DPO, autorizzati)
4. cooperazione con il Garante,
5. segretezza (art. 90, autonomia Stato membro).

Il titolare del trattamento

CAMBIA	• Obblighi, diritti e poteri ampliati • Prevista espressamente la **"contitolarità" (art. 26) con necessità di atti giuridicamente validi** in cui definire responsabilità e compiti di ciascun titolare con particolare riguardo all'esercizio dei diritti degli interessati. • Designa un responsabile del trattamento **con contratto** o analogo atto attribuendogli **specifici compiti** (almeno le materie al paragrafo 3 dell'art. 28). • Designa il DPO.
NON CAMBIA	• Il Regolamento individua caratteristiche soggettive e responsabilità del titolare

CENTRO NAZIONALE SANGUE

Il responsabile del trattamento

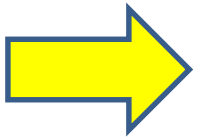
• Figura già prevista ma rinnovata, può essere un interno all'organizzazione del titolare o esterno (sicuramente lo sono i fornitori).
• Deve avere conoscenza specialistica, affidabilità e risorse
• Deve essere istruito dal titolare.
• Non è una figura necessaria.

Obblighi:

1. mette in atto misure tecniche e organizzative rispondenti ai requisiti del Regolamento,
2. tiene il registro delle attività,
3. garantisce la riservatezza degli autorizzati,
4. se non si attiene alle istruzioni del titolare diviene titolare,
5. designa il DPO.

Il responsabile del trattamento

CAMBIA	• **Obblighi specifici diversi** da quelli del titolare (registro dei trattamenti, designazione DPO) • Può nominare un **sub-responsabile** per specifiche attività di trattamento per il quale risponde in caso di inadempienza.
NON CAMBIA	• Il Regolamento individua caratteristiche soggettive e responsabilità del Responsabile.



Necessario verificare conformità degli attuali contratti con i Responsabili del trattamento all'art. 28, se del caso modificare/aggiornare. Previsti modelli di clausole contrattuali ad opera del Garante nazionale.

CENTRO NAZIONALE SANGUE

Data protection officer (DPO)

- Nuova figura volta a **facilitare l'attuazione del regolamento** da parte del titolare/responsabile.
- Costituisce una **misura organizzativa** obbligatoria in alcuni casi, sempre consigliata.
- Designazione del Titolare o del Responsabile o di entrambi congiuntamente r notifica al Garante.
- Deve avere **indipendenza**, **autorevolezza**, **competenze manageriali** e risorse adeguate.
- Può essere figura interna o esterna all'organizzazione o società, con cui è necessario sottoscrivere **formale contratto**.
- Non è il destinatario degli obblighi del Regolamento ma…
- Ha compiti di: **consulenza**, **vigilanza**, **garanzia**.

Più titolari/responsabili possono condividere uno stesso DPO purchè il DPO risulti comunque efficiente.

DPO: criteri di designazione

TRATTAMENTO IN AMBITO PUBBLICO

↓

DESIGNAZIONE OBBLIGATORIA

TRATTAMENTO IN AMBITO PRIVATO

↓

Trattamento attività principale

↓

Trattamento su larga scala

↓

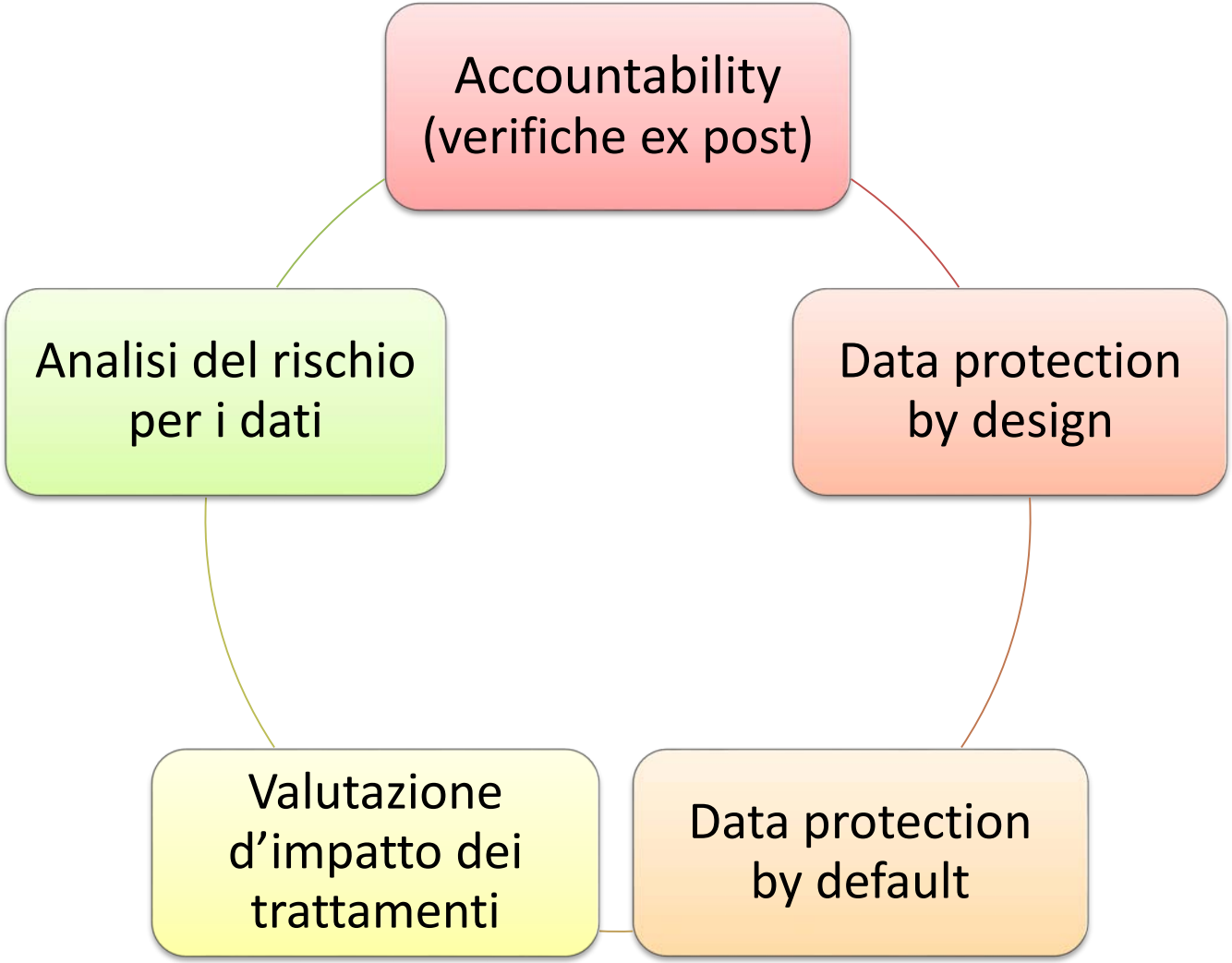
Tr. regolare o costante **o** Tr. di dati particolari

↓

DESIGNAZIONE OBBLIGATORIA

CENTRO NAZIONALE SANGUE

Approccio basato sul rischio e misure di accountability di titolari e responsabili - 1

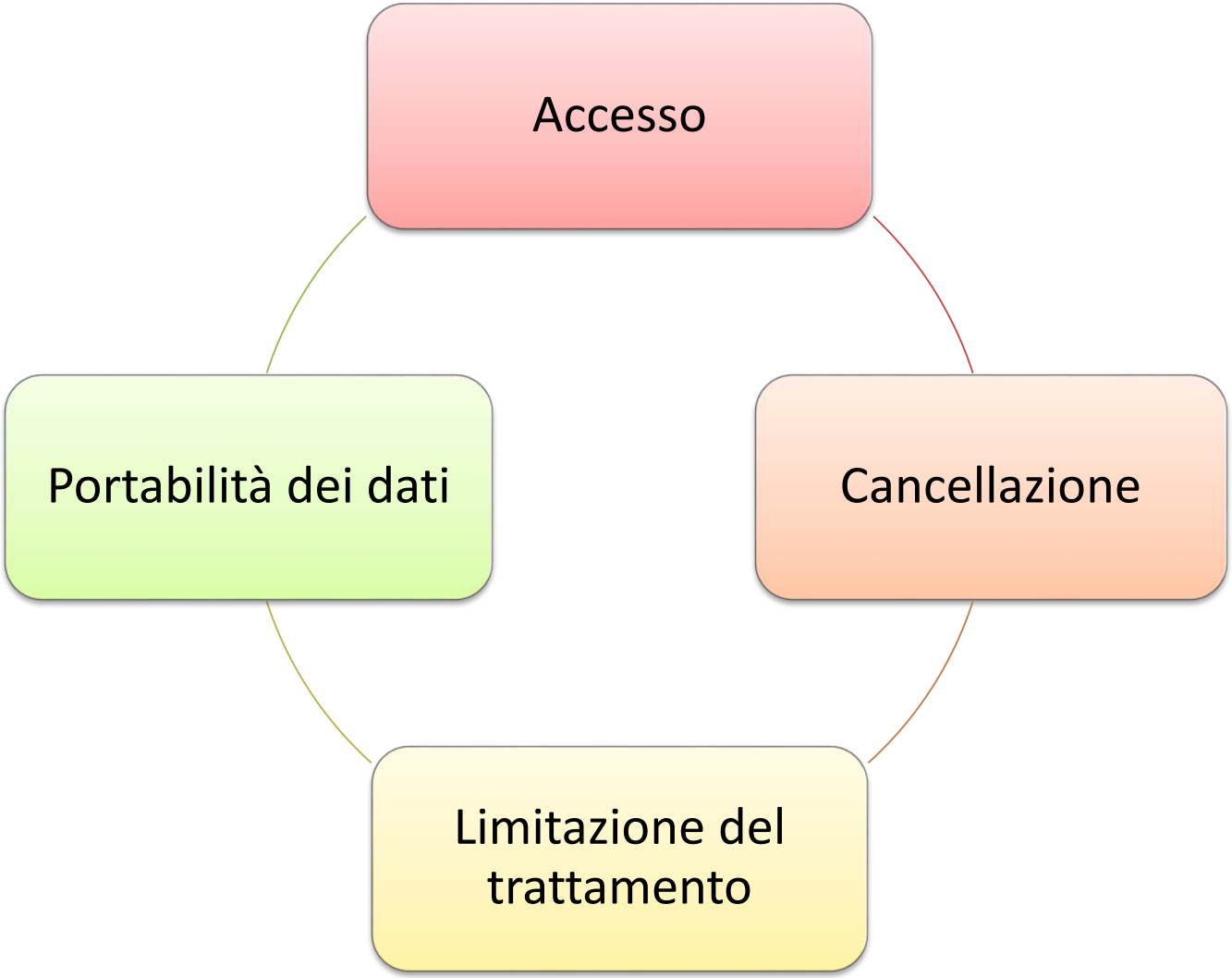


Approccio basato sul rischio e misure di accountability di titolari e responsabili - 2

Il Registro dei trattamenti (art. 30)

- Ad opera di titolari e i responsabili di trattamento,
- Eccezione: gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, il trattamento è occasionale e non si applica a dati particolari
- Il primo passo per ogni valutazione e analisi del rischio
- Da tenere in forma scritta, anche elettronica, da esibire su richiesta al Garante

Approccio basato sulla garanzia dei diritti degli interessati



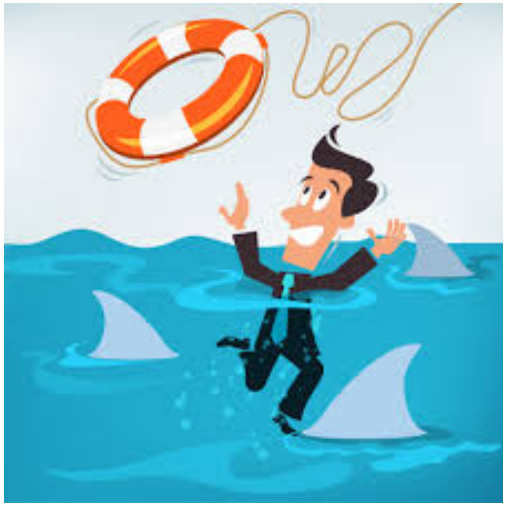
SOS PRIVACY

CODICI DI CONDOTTA

LINEE GUIDA INTERNAZIONALI

CERTIFICAZIONI

MODELLI NAZIONALI



GIURISPRUDENZA DEL GARANTE

CENTRO NAZIONALE SANGUE

www.garanteprivacy.it

CENTRO NAZIONALE SANGUE

Grazie dell'attenzione!