PROTEZIONE DEI DATI PERSONALI NELLA RICERCA CLINICA

16 GENNAIO 2019

MARINA SALOMONI
UNITA'RICERCA CLINICA
ISTITUTO ONCOLOGICO VENETO

Dichiarazione di Helsinki
Good Clinical Practice (GCP)

Tutela dei diritti dei soggetti che partecipano ad una ricerca biomedica:

- Diritto al benessere, sicurezza ed integrità
- Diritto all'informazione ed alla tutela della riservatezza dei dati

Le informazioni sulle garanzie a tutela della Privacy sono parte integrante del processo del CONSENSO INFORMATO
destinato ai soggetti che partecipano ad una ricerca clinica

Dichiarazione di Helsinki (Ed. 2013)

…

24. Devono essere predisposte tutte le azioni finalizzate **a garantire la privacy dei soggetti coinvolti nella ricerca e la riservatezza dei loro dati personali.**

32. Per la ricerca biomedica che utilizza dati identificabili o campioni biologici di origine umana, contenuti in bio-banche o in simili depositi, i medici devono acquisire il consenso informato per la loro raccolta, lo stoccaggio e/o il riutilizzo. Nelle **situazioni eccezionali in cui è impossibile o impraticabile ottenere il consenso**, la ricerca può essere avviata solo dopo **valutazione e approvazione del Comitato Etico.**

Good Clinical Practice (GCP)

GLOSSARIO … 1.16 Confidenzialità
Evitare, se non a persone autorizzate, la divulgazione di informazioni di proprietà dello sponsor **o riguardanti l'identità del soggetto.**

PRINCIPI di GCP/ICH … 2.11 Deve essere garantita la riservatezza dei documenti che potrebbero identificare i soggetti, rispettando le regole di riservatezza e confidenzialità previste dalle disposizioni normative applicabili

5.15.2 Lo sponsor deve accertarsi che ogni soggetto abbia acconsentito per iscritto all'accesso diretto alla propria documentazione clinica originale per il monitoraggio, audit, revisione, ispezioni.

]

Regolamento EU 536/2014 – Art. 56

Registrazione, elaborazione, gestione e conservazione delle informazioni

1. Tutte le informazioni sulla sperimentazione clinica sono registrate, elaborate, gestite e conservate dal promotore o dallo sperimentatore, a seconda dei casi, in modo tale da poter essere comunicate, interpretate e verificate in modo preciso, tutelando al tempo stesso **la riservatezza dei dati e i dati personali dei soggetti in conformità del diritto applicabile in materia di protezione dei dati personali.**

2. Sono attuate idonee misure tecniche e organizzative per tutelare le informazioni e i dati personali trattati, da rivelazione, diffusione, modifica non autorizzati o illeciti, o dalla distruzione o perdita accidentale, in particolare quando il trattamento comporta la trasmissione attraverso una rete telematica

Normativa Privacy in vigore **fino al 24 Maggio 2018**

- **Decreto Legislativo n. 196 del 30 Giugno 2003**
- **Deliberazione n. 52 del 24 Luglio 2008**: "Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali.»
- **Autorizzazioni del Garante Privacy** per Genetica e Sperimentazione clinica (rinnovate annualmente);

Normativa Privacy **dal 25 Maggio 2018**

- **GDPR n. 679/2016**
- **Decreto Legislativo n. 196 del 30 Giugno 2003 modificato dal Decreto Legislativo n. 101 del 10 Agosto 2018** (recepimento del GDPR 679/2016)
- **Provvedimento n. 497 del 13 .12.2018** del Garante della Privacy

GDPR (General Data Protection Regulation)
REGOLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
(27 Aprile 2016)

«La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un DIRITTO FONDAMENTALE»

Il GDPR rappresenta un insieme di principi e di norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali, che sono valide per tutti i Paesi dell'UE.

E' costituito da 173 Considerando e da 99 Articoli

Art. 99

1. «Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

2. Esso si applica a decorrere da 25 maggio 2018.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

GDPR

I PRINCIPALI CONTENUTI

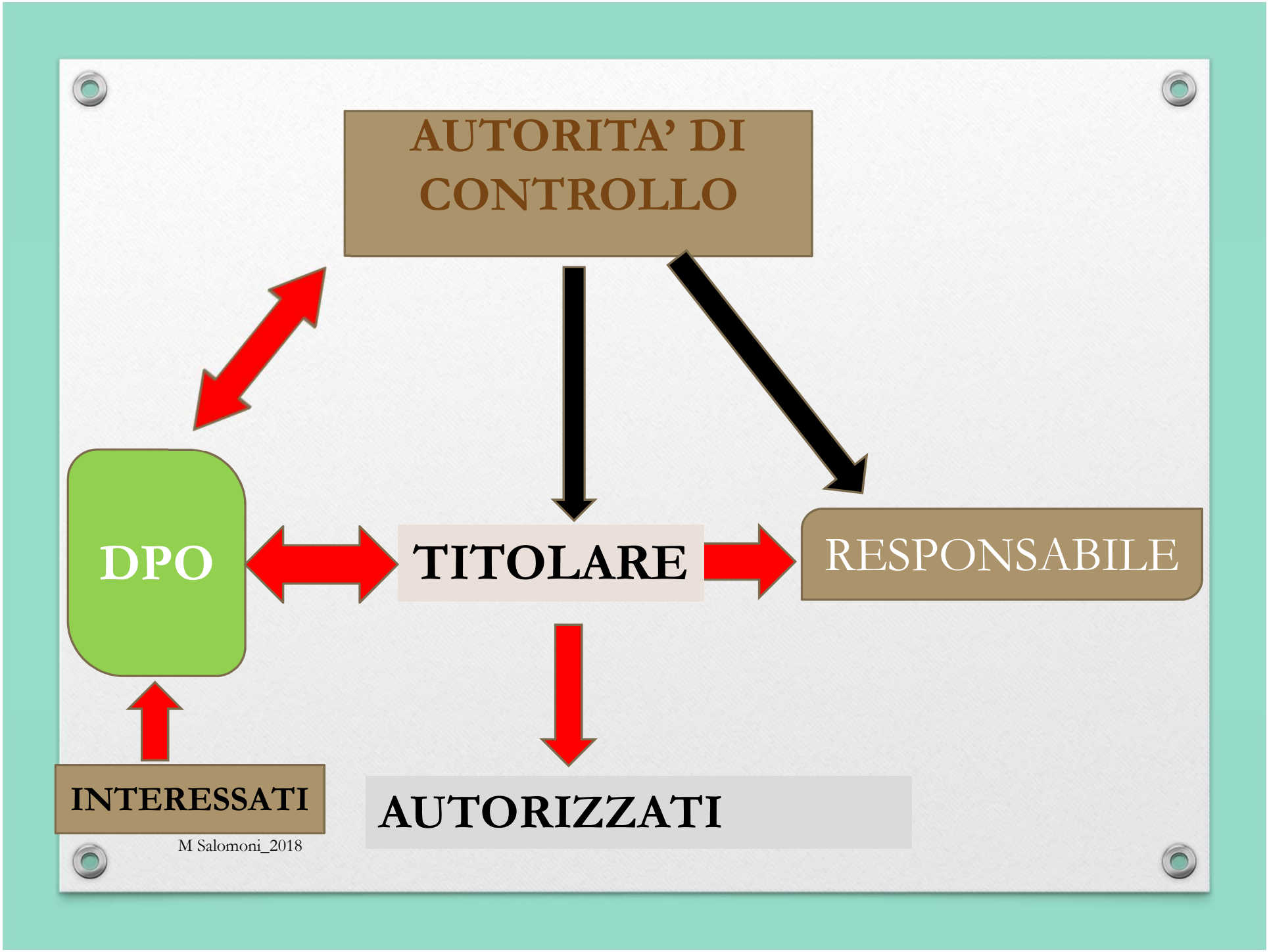
1. **Identifica gli ATTORI COINVOLTI nel processo di trattamento dei dati.**
2. **Introduce il principio di RESPONSABILIZZAZIONE del titolare**
3. **Fornisce MODALITA' (quando? Come?) e CONTENUTI per un'INFORMAZIONE ADEGUATA da somministrare al soggetto interessato per l'acquisizione del CONSENSO volontario e consapevole al trattamento dei dati (Art. 13 e 14)**

GDPR

4. **Indica le MISURE IDONEE per trattare i dati con il minimo rischio di violazione.**

5. **APPARATO SANZIONATORIO (Art 83, 84)**

   Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento.


AUTORITA' DI CONTROLLO
DPO
TITOLARE
RESPONSABILE
INTERESSATI
AUTORIZZATI
M Salomoni_2018

GDPR - DEFINIZIONI

TITOLARE del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le FINALITA' e i MEZZI del trattamento di dati personali

RESPONSABILE del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

ACCESSO non autorizzato ai dati	Personale non autorizzato (esterno/interno)	Archiviazione sicura dei documenti cartacei Configurazione di profili di accesso alle Banche-dati	Riservatezza
PERDITA di dati	Malfunzionamento, degrado dei sistemi informatici Azione di virus informatici Incuria, carenza di consapevolezza	Adeguamento di misure di back-up dei dati Programmi antivirus Formazione del personale, adeguamento di istruzioni operative	Integrità
MODIFICHE non autorizzate di dati	Incuria, carenza di consapevolezza	Formazione del personale, adeguamento di istruzioni operative	Integrità
DIVULGAZIONE di dati	Pubblicazione o invio di dati personali	Formazione del personale, adeguamento di istruzioni operative	Riservatezza

VIOLAZIONE DEI DATI PERSONALI – GDPR Art. 33

NOTIFICA ALL'AUTORITA' DI CONTROLLO

- **In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza.**

- **In quali casi?**

- **quando la violazione dei dati personali presenti un rischio ELEVATO per i diritti e le libertà delle persone fisiche.**

- **Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.**

TITOLARE

Sono ampliati gli obblighi in materia di tutela dei dati personali, al fine non solo di garantire il rispetto delle norme fissate per il trattamento dei dati personali, ma anche di RESPONSABILIZZAZIONE, che implica di

1. **adottare e dimostrare di aver adottato una serie di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali**
2. **ma anche assicurare una continua ATTIVITA' DI CONTROLLO E VERIFICA delle proprie attività di trattamento**

COMPITI del DPO – Art. 38

1. **Informare e fornire consulenza al titolare nonché ai DIPENDENTI che eseguono il trattamento, sull'applicazione del Regolamento;**
2. **Sorvegliare l'osservanza del GDPR da parte del titolare, compresa ad es. la sensibilizzazione e la formazione del personale che partecipa ai trattamenti**
3. **Essere PUNTO di CONTATTO per Garante ed interessati che lo possono contattare per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti**

TITOLARE - OBBLIGHI

1. LICEITA' DEL TRATTAMENTO
2. MINIMIZZAZIONE
3. CONSERVAZIONE
4. INFORMAZIONE AGLI INTERESSATI distinta (quando? come?)
5. Designazione del DPO (interno, esterno)
6. NOTIFICA DI VIOLAZIONE (rischio elevato)

STRUMENTI

1. REGISTRO DEI TRATTAMENTI
2. VALUTAZIONE D'IMPATTO DEI RISCHI
3. DPO
4. UFFICIO PRIVACY INTERNO (non prescritto)

GDPR – DPO
Il titolare designa il DPO

Il titolare si assicura che

- **il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali**

- **Gli siano fornite le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.**

GDPR - DEFINIZIONI

Nel Regolamento EU viene ampliata la definizione di DATO PERSONALE e SENSIBILE
Sono individuate 4 categorie di dati:
DATI PERSONALI, DATI GENETICI,
DATI BIOMETRICI, DATI SULLA SALUTE.

ART 4 - DATI PERSONALI: qualsiasi informazione riguardante una persona fisica identificata o identificabile (che può essere identificata, direttamente o indirettamente, es. un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno

GDPR - DEFINIZIONI

più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale).

GDPR - Articolo 9

Trattamento di CATEGORIE PARTICOLARI DI DATI PERSONALI

1. **È 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**
2. **Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:**
   a) **l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche .**

...

GDPR - Articolo 9

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o …

ed è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

…

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

D.Lgs 101/2018 – Art 110

Il consenso **non è inoltre necessario** quando, a causa di particolari ragioni, informare gli interessati **risulta impossibile o implica uno sforzo sproporzionato**, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi,

1. il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato,
2. il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e
3. deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.

INFORMATIVA E MANIFESTAZIONE DEL CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Deliberazione n. 52 del 24 Luglio 2008: “Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali.»

- ALLEGATO: modello di informativa
- Indica contenuti e modalità di somministrazione dell’informativa

OGGI?

CONTENUTI DELLE INFORMAZIONI AGLI INTERESSATI
GDPR ARTICOLI 13, 14 e 15

1. <u>INFORMAZIONI</u>

Titolo dello studio

Nome, indirizzo del Centro clinico (titolare dei dati)

Nome, indirizzo del Promotore (co-titolare dei dati)

Finalità del trattamento (a che fine vengono raccolti i dati)

Natura dei dati (quali dati verranno raccolti e trattati)

Base giuridica del trattamento (che cosa rende legittimo il trattamento)

Natura e conseguenze del trattamento (se la persona è obbligata o meno a conferire i propri dati e cosa succede se non conferisce i dati)

Modalità del trattamento dei dati (come vengono raccolti e trattati i dati)

Comunicazione e diffusione (a chi potranno essere comunicati i dati personali)

Durata del trattamento (per quanto tempo vengono conservati i dati)

Esercizio dei diritti

Recapiti DPO dei titolari e del Garante della Privacy (reclamo).

Consenso al trasferimento dei dati personali in Paesi terzi ed elenco dei Paesi (ove applicabile)

2. <u>CONSENSO</u>

Nome e cognome dell'interessato/di chi esercita la responsabilità genitoriale/del rappresentante legale/testimone imparziale

…E PER I CONSENSI ACQUISITI PRIMA DEL GDPR?

Considerando 171

Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento.

GDPR – Considerando 50

…E L'UTILIZZO DI DATI PER RICERCHE FUTURE (senza consenso)?

Il trattamento dei dati personali **per FINALITA' DIVERSE** da quelle per le quali i dati personali sono stati inizialmente raccolti **dovrebbe essere consentito solo se COMPATIBILE con le finalità** per le quali i dati personali sono stati inizialmente raccolti. In tal caso **non è richiesta alcuna base giuridica separata** oltre a quella che ha consentito la raccolta dei dati personali.

- **L'ulteriore trattamento a fini di** archiviazione nel pubblico interesse, o **di ricerca scientifica** o storica o a fini statistici dovrebbe essere considerato un **trattamento lecito e compatibile.** La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento**.**

Decreto Legislativo n.101 del 10.08.2018 che modifica ed integra il D. Lgs 196/2003

«Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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(regolamento generale sulla protezione dei dati).»

Si tratta del decreto legislativo che aggiorna il D. Lgs 196/2003 (codice della Privacy) che rimane in vigore (anche se molti articoli vengono abrogati o modificati sostanzialmente dal decreto 101)

Stabilisce che l'Autorità di controllo sulla privacy in Italia è (o meglio rimane) l'Autorità Garante per la protezione dei dati personali

D. Lgs 196/2003 e D. Lgs 101/2018 rappresentano fonti normative sotto-ordinate rispetto al GDPR

il Codice rappresenta una forma di "adeguamento" alle superiori disposizioni comunitarie.

Il Garante stabilisce misure di garanzia con un provvedimento, sottoposto a consultazione popolare (Codice deontologico)

… E QUANDO SI TRATTA DI MINORI?

GDPR - Considerando 38: I minori meritano una

specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali.

… Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori **a fini di marketing…**

D. Lgs.101/2018 – Art. 2-quinquies: Consenso del minore in relazione ai servizi della società dell'informazione

In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i **14 anni** può esprimere il consenso al trattamento dei propri dati personali

GDPR

Il linguaggio deve essere particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo.

In tutti gli altri casi (minori di età < 14 anni e in tutti gli altri ambiti con età < 18 anni) il consenso viene prestato da chi esercita la responsabilità genitoriale