GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

T4DATA

In collaborazione con
REGIONE MARCHE

EVENTO FORMATIVO SUL RGPD
REGOLAMENTO (UE) 2016/679

Il trattamento dei dati personali per finalità di cura e ricerca

7 giugno 2019

Auditorium Tamburi
Mole Vanvitelliana
Banchina Giovanni da Chio, 28 - Ancona

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

T4DATA

In collaborazione con
REGIONE MARCHE

EVENTO FORMATIVO SUL RGPD
REGOLAMENTO (UE) 2016/679

Il trattamento dei dati personali per finalità di cura e ricerca

Assessore regionale *Fabrizio Cesetti*

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4DATA

In collaborazione con REGIONE MARCHE

EVENTO FORMATIVO SUL RGPD

REGOLAMENTO (UE) 2016/679

Il trattamento dei dati personali per finalità di cura e ricerca

Presentazione del progetto T4DATA

Antonio Caselli
Segreteria generale del Garante

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

T4DATA

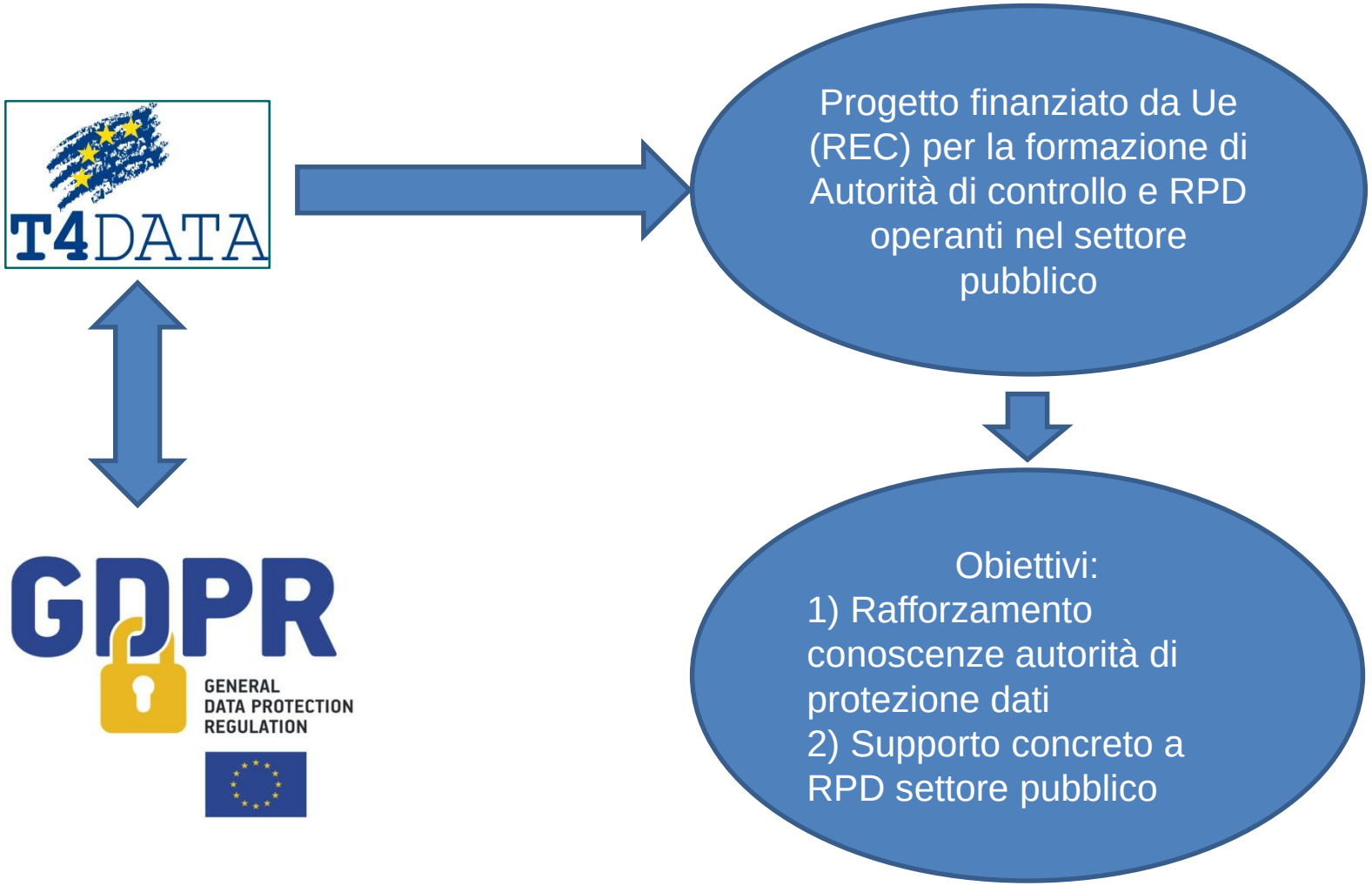
Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

T4Data – Il progetto

Antonio Caselli

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Il progetto T4Data



T4Data: «Deliverables»

I FASE: 2018
Formazione **Autorità di controllo**
Workshops, Seminari, **Manuale RPD**

II FASE: 2019
Formazione **RPD**
Webinar ad-hoc, **Seminari locali**

Final Conference (Roma)

III FASE: Post-2019
Diffusione contenuti a livello nazionale
Iniziative di sensibilizzazione

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4Data: I seminari locali di formazione

https://www.garanteprivacy.it/regolamentoue/formazione/t4data

Ancona	Catanzaro 26 giugno	Torino 1 ottobre	Roma I metà novembre
Sanità e ricerca	Trasparenza, accesso, *big data*	Sicurezza e gestione del rischio	Responsabilità sanzioni

Approfondimento tematiche specifiche + Casi pratici + Q&A

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

T4Data: I webinar di formazione

https://www.garanteprivacy.it/regolamentoue/formazione/t4data

Piattaforma **dedicata** web-based + **Webinar** preregistrati + Materiali di supporto

Modulo I	Modulo II	Modulo III	Modulo IV
I fondamentali della protezione dati	RPD: Ruoli, responsabilità	Un toolkit per l'RPD (how-to)	Approfondimenti specifici

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

T4Data

https://www.garanteprivacy.it/regolamentoue/formazione/t4data

GDPR ⟺ G RPD

Buon lavoro a tutti e grazie

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4DATA

In collaborazione con REGIONE MARCHE

EVENTO FORMATIVO SUL RGPD

REGOLAMENTO (UE) 2016/679

Il trattamento dei dati personali per finalità di cura e ricerca

Sanità tra tecnologia e gestione del rischio (Valutazione di impatto, DPO e registro delle attività di trattamento)

Francesco Modafferi
Dirigente Dipartimento realtà pubbliche
e Dipartimento sanità e ricerca

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

Sanità tra tecnologia e gestione del rischio

Francesco Modafferi

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Dove eravamo rimasti?

Il Garante incontra i Responsabili della Protezione dei Dati

Prime indicazioni per l'attuazione dei compiti e per la definizione delle modalità di relazione con l'Autorità

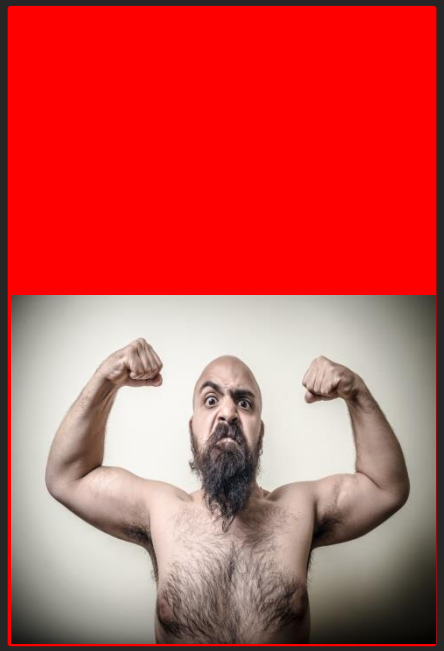
24 maggio 2018

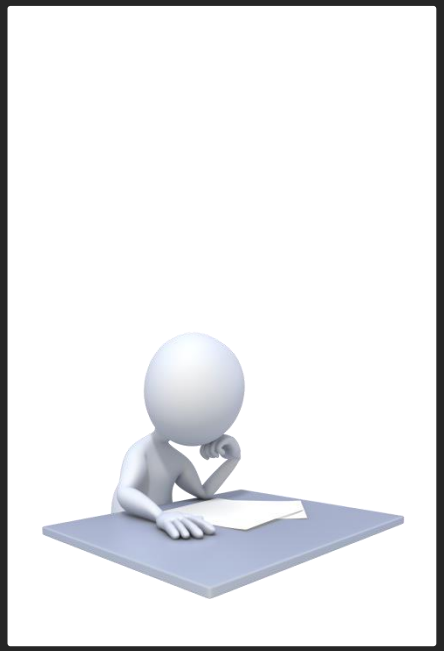
Palazzo dei Congressi
Piazza della Costituzione, 4 - Bologna

All'incontro saranno presenti tutti i Componenti del Collegio dell'Autorità Garante

9.00 - *Registrazione dei partecipanti*


Eurobarometro
RPD





Il sondaggio

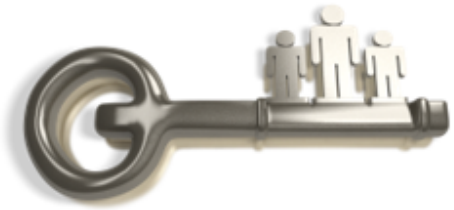
T4DATA

Sondaggio

La cosa di cui sento più bisogno

(barrare la casella –una sola- che indica la risorsa di cui si avverte il maggior bisogno):

☐	Risorse economiche
☐	Personale
☐	Tempo
☐	Formazione propria
☐	Strumenti per formare gli altri
☐	Scambio di esperienze con altri RPD
☐	Riviste specializzate in materia di protezione dei dati personali
☐	Altro (specificare):



Cosa è successo nel frattempo?

Regole deontologiche

Entro novanta giorni dalla data di entrata in vigore del decreto, il Garante verifica la conformità al dei seguenti Codici:

Allegato A.1. - Codice di deontologia - Trattamento dei dati personali nell´esercizio dell´attività giornalistica

Allegato A.2. - Codice di deontologia - Trattamento dei dati personali per scopi storici

Allegato A.3. - Codice di deontologia - Trattamento dei dati personali a scopi statistici in ambito Sistan

Allegato A.4. - Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici

Allegato A.6. - Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive

Le disposizioni ritenute compatibili, rinominate regole deontologiche, sono pubblicate nella Gazzetta Ufficiale e, con decreto del Ministro della giustizia, sono successivamente riportate nell'allegato A del codice

Autorizzazioni generali

Il Garante, con provvedimento di carattere generale da porre in consultazione pubblica entro novanta giorni dalla data di entrata in vigore del decreto

individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative ai trattamenti di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del regolamento, che risultano con esso compatibili e, ove occorra, provvede al loro aggiornamento

Il provvedimento è adottato entro sessanta giorni dall'esito del procedimento di consultazione pubblica.

Le autorizzazioni generali sottoposte a verifica che sono state ritenute incompatibili con il Regolamento cessano di produrre effetti dal momento della pubblicazione del provvedimento

Sino all'adozione delle regole deontologiche e delle misure di garanzia di cui agli articoli 2-quater e 2-septies del Codice, le autorizzazioni generali e le prescrizioni individuate con il provvedimento di cui sopra producono effetti, per la corrispondente categoria di dati e di trattamenti.

I chiarimenti del Garante

Provvedimento del 7 marzo 2019

I nuovi regolamenti sui procedimenti dell'Autorità

Regolamento n 1/2019

Deliberazione del 4 aprile 2019 - Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali [9107633]

[doc. web n. 9107633]

Deliberazione del 4 aprile 2019 - Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali
(Pubblicato sulla Gazzetta Ufficiale n. 106 dell'8 maggio 2019)

Registro dei provvedimenti
n. 98 del 4 aprile 2019

Regolamento n 2/2019

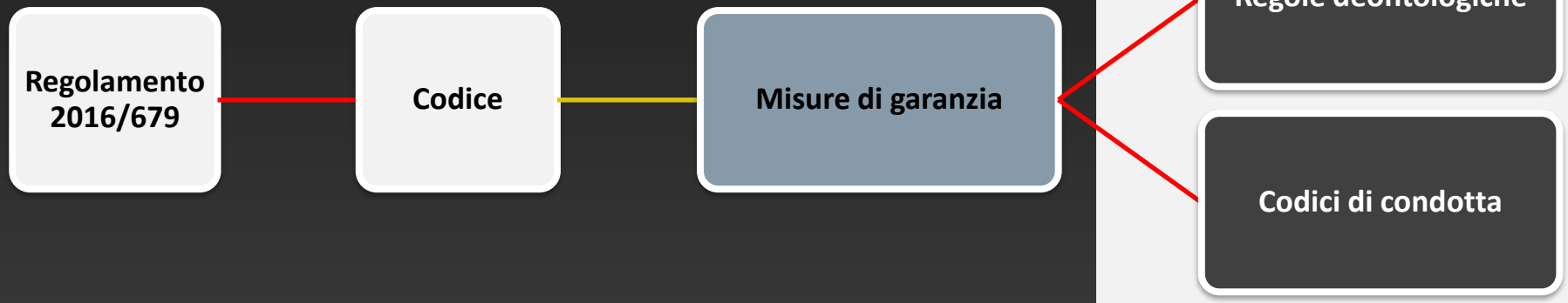
Deliberazione del 4 aprile 2019 - Regolamento n. 2/2019, concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali [9107640]

[doc. web n. 9107640]

Deliberazione del 4 aprile 2019 - Regolamento n. 2/2019, concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi presso il Garante per la protezione dei dati personali
(Pubblicato sulla Gazzetta Ufficiale n. 107 del 9 maggio 2019)

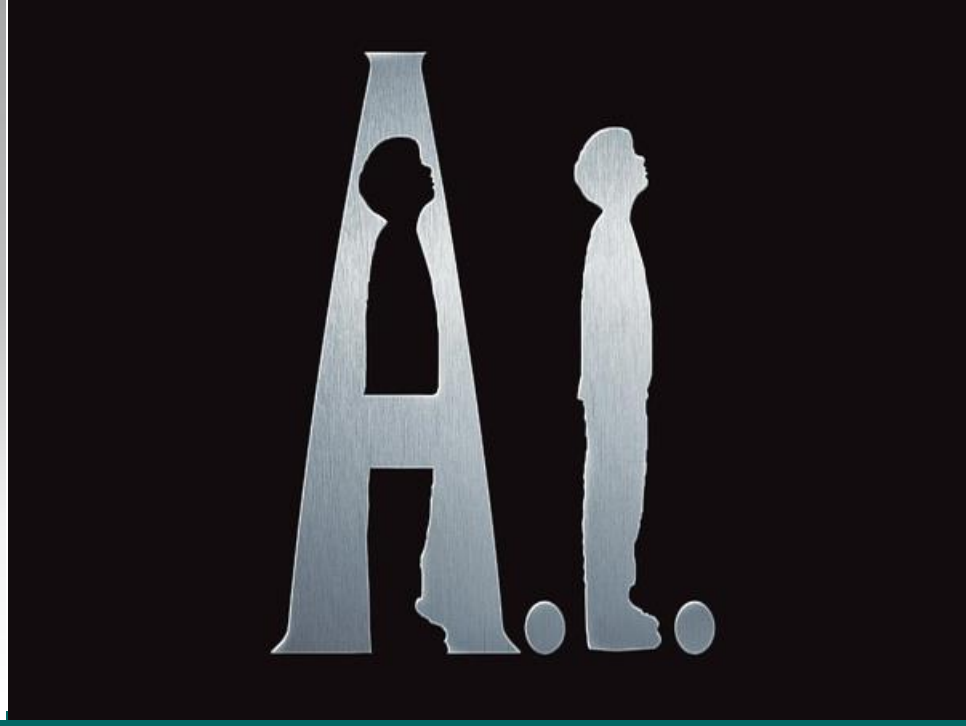
Registro dei provvedimenti
n. 99 del 4 aprile 2019

Il quadro regolatorio a regime



Regolamentazione

Auto -regolamentazione

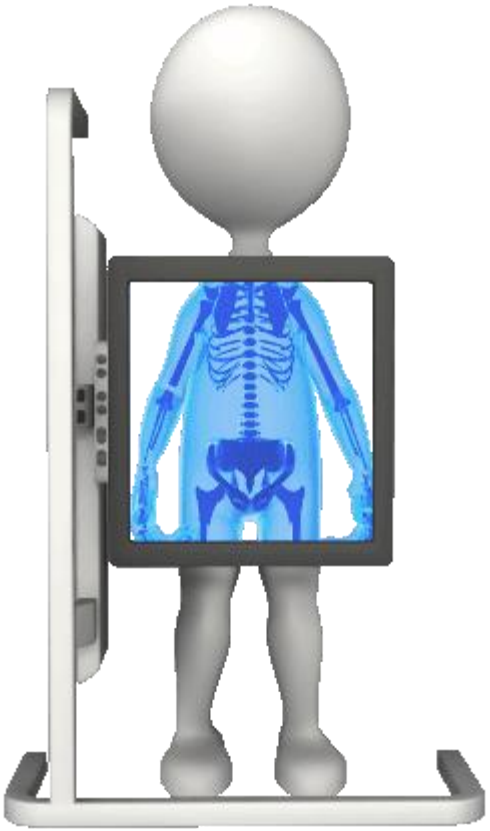


I trattamenti dati nel contesto sanitario e della ricerca scientifica oggi

Big data

Prendersi cura del paziente oggi…

..significa prendersi cura anche dei suoi dati



In ambito medico l'osservanza delle disposizioni relative al trattamento dei dati sono rilevanti non solo ai fini dell'applicazione della disciplina di settore (Codice privacy), ma anche del rispetto del Codice di deontologia medica.

(art. 11 Riservatezza dei dati personali, 12 Trattamento dei dati sensibili, 25 Documentazione sanitaria, 26 Cartella clinica, 34 Informazione e comunicazione a terzi, 78 Tecnologie informatiche)

Data value cycle

Gli effetti collaterali latenti del trattamento

- Come rilevato da Ulrich Beck, l'evoluzione tecnologica va di pari passo con la produzione sociale di rischi; uno degli obiettivi di fondo della regolazione è dunque quello di gestire i cc.dd. "effetti collaterali latenti" di questa evoluzione per "*limitarli e diluirli distribuendoli in modo che non ostacolino il processo di modernizzazione né travalichino i confini di ciò che è considerato* ***'tollerabile'***".
- In questo contesto, il Regolamento introduce nuove **garanzie** proprio per far fronte ai rischi che possono derivare dal trattamento dei dati personali.

4 Considerando

Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, IN OSSEQUIO AL PRINCIPIO DI PROPORZIONALITÀ. Il regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

6 e 7 | Considerando

La rapidità dell'evoluzione tecnologica comporta nuove sfide per la protezione dei dati personali. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività

Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno.

È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche

Risk based approach

Il rischio in materia di protezione dei dati personali è la possibilità che a causa di un trattamento si possa produrre un effetto negativo sui diritti e sulle libertà delle persone coinvolte

Tale possibile ricaduta negativa, seppure non voluta o desiderata dal titolare, deve comunque essere considerata, valutata e gestita

I presupposti della DDI

Quando le informazioni sono condivise aumentano i rischi connessi alla sicurezza

Quando i dati sono collegati ad altri (big data) la risultante che ne deriva comporta un maggior grado di conoscenza delle informazioni dell'interessato

I danni potenziali che possono derivare dal trattamento illecito dei dati personali possono essere molto gravi sia dal punto di vista patrimoniale che non patrimoniale (discriminazioni nei rapporti con le assicurazioni o sul luogo di lavoro, stigmatizzazione e perdita di reputazione, stress)

Occorre quindi considerare con grande attenzione il rischio della perdita di fiducia nei confronti delle istituzioni e del sistema sanitario che può derivare

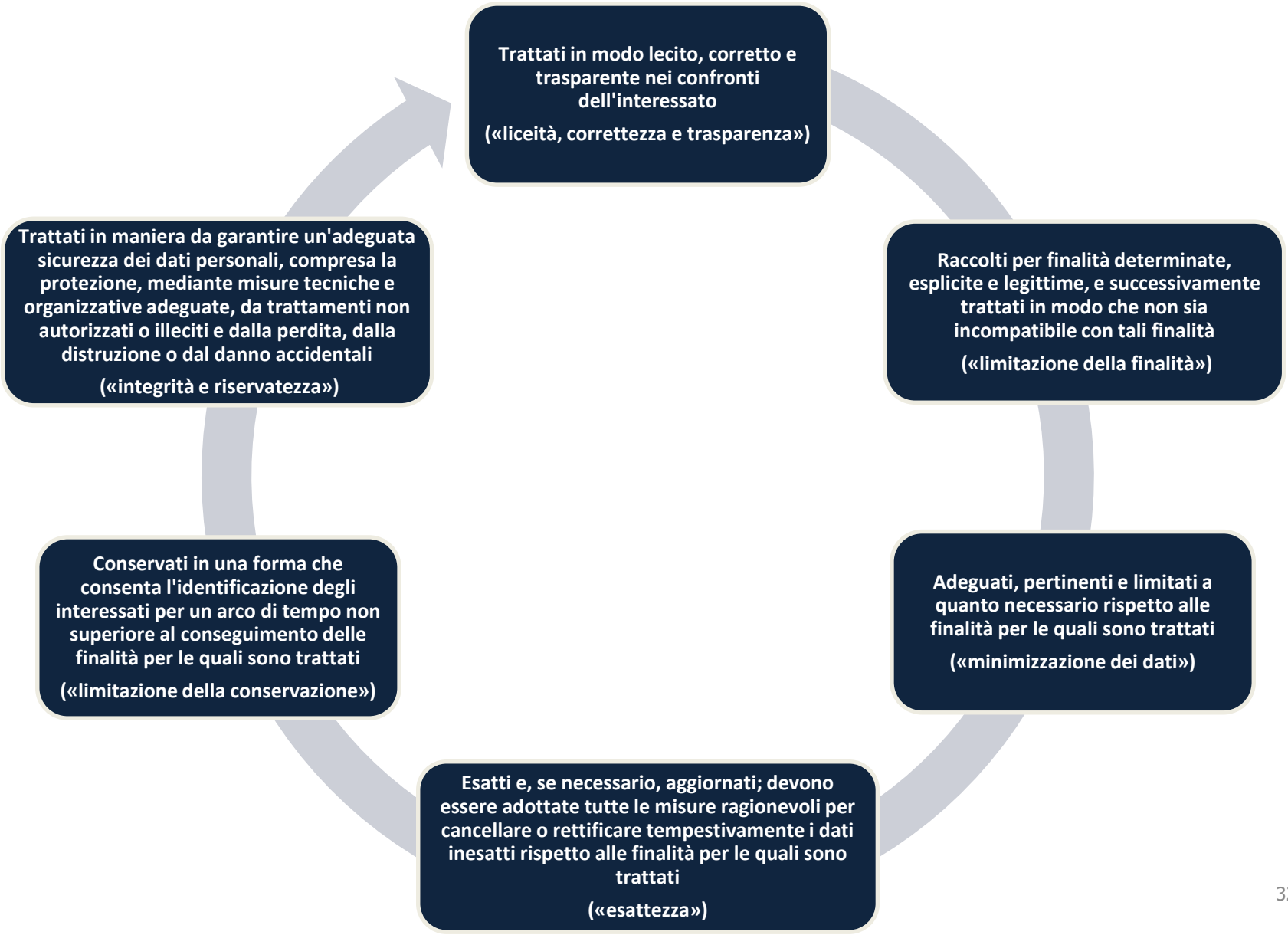
Riflessione troppo modesta sulle conseguenze per le persone nel medio – lungo periodo

La nostra missione è ricercare un approccio responsabile perchè dietro i dati ci sono le persone

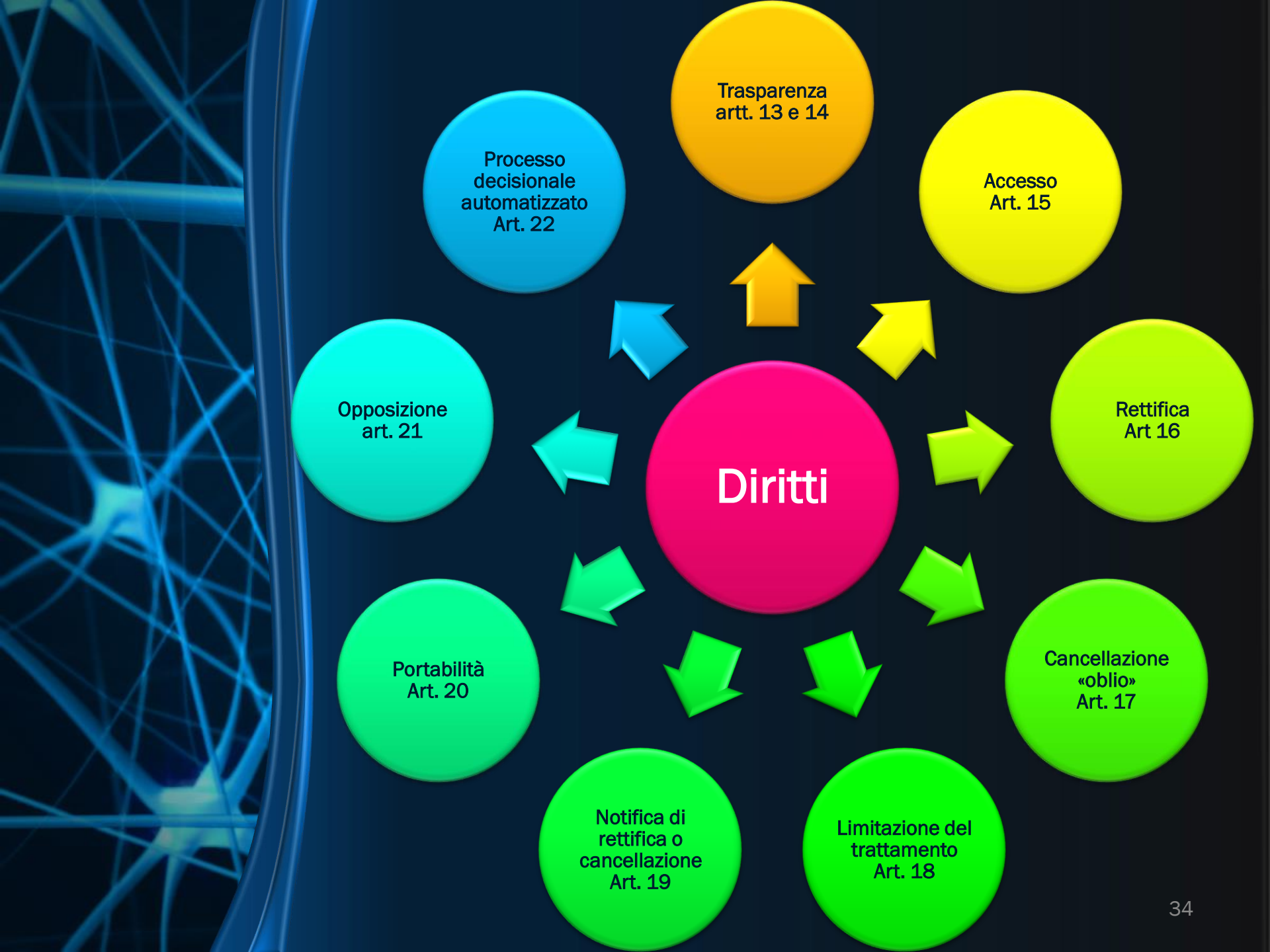
Occorre un cambio radicale di prospettiva

Le 3 cose che contano (veramente!)

Il punto di partenza: i principi generali del trattamento

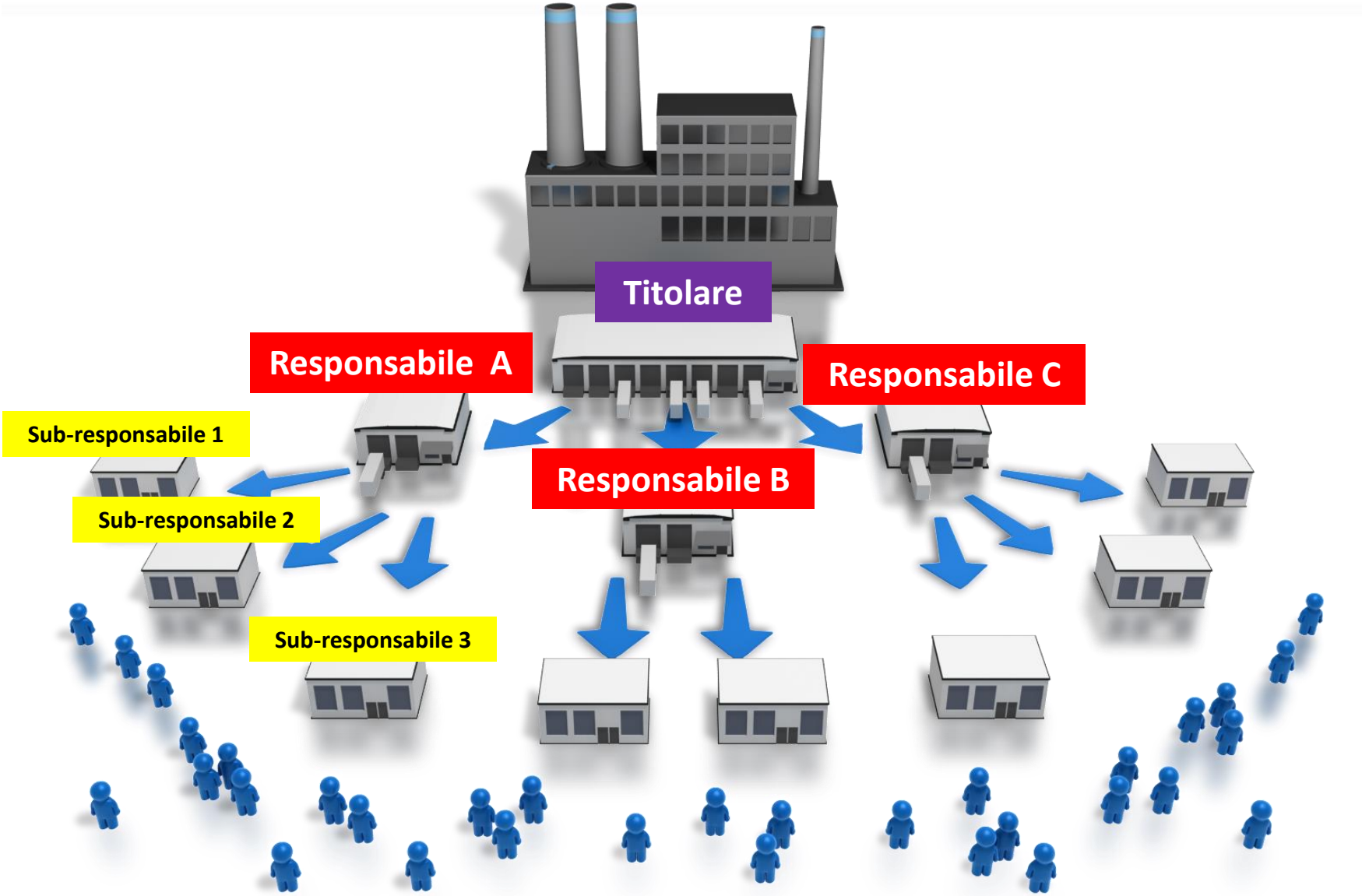



VISITA DI CONTROLLO DEL TRATTAMENTO
LICEITÀ:
Quale è la base giuridica in funzione della quale effettuiamo il trattamento?
TRASPARENZA:
Abbiamo previsto le modalità attraverso le quali informare l'interessato sul trattamento?
CORRETTEZZA:
C'è congruenza tra quanto prospettato all'interessato e il trattamento che faremo?
FINALITÀ:
Quali sono le finalità, per le quali i dati sono trattati?
MINIMIZZAZIONE:
I dati che tratteremo sono adeguati, pertinenti e limitati a quanto necessario rispetto alle nostre finalità?
ESATTEZZA:
Abbiamo previsto tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ?
CONSERVAZIONE:
Abbiamo previsto che i dati siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità?
INTEGRITÀ E RISERVATEZZA:
Abbiamo adottato misure tecniche e organizzative adeguate per proteggere i dati da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali?


Diritti
Trasparenza artt. 13 e 14
Accesso Art. 15
Rettifica Art 16
Cancellazione «oblio» Art. 17
Limitazione del trattamento Art. 18
Notifica di rettifica o cancellazione Art. 19
Portabilità Art. 20
Opposizione art. 21
Processo decisionale automatizzato Art. 22


I ruoli
del trattamento

Il trattamento effettuato «per conto» del titolare



Nuove linee guida su titolare-responsabile

Guidelines nr/year on topic the concepts of controller and processor in the GDPR – update of Art 29 WP opinion 1/2010


Accountability

L’algoritmo dell’accountability

Tenuto conto

della natura

dell'ambito di applicazione

del contesto

delle finalità del trattamento

dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

il titolare del trattamento mette in atto misure

tecniche

organizzative

adeguate per

garantire

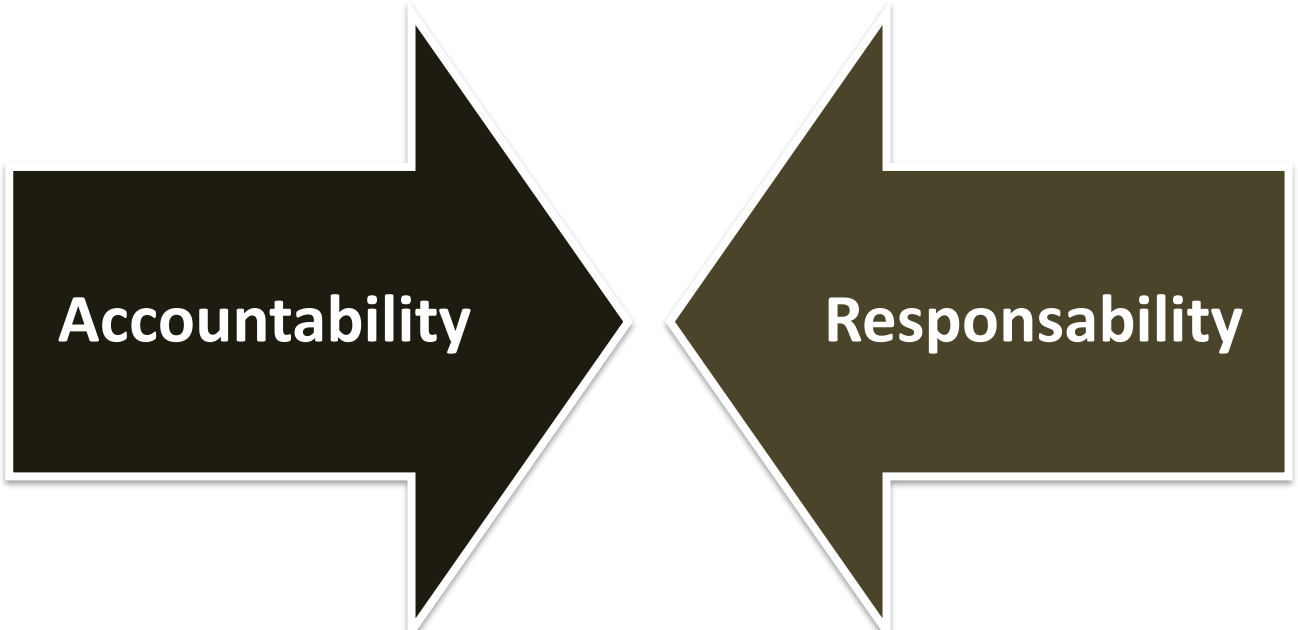
ed essere in grado di dimostrare

che il trattamento è effettuato conformemente al regolamento

L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Il RPD elemento dell'accontability

Il RPD rappresenta il mezzo principale per mettere in pratica il principio di responsabilizzazione (accountability) nel settore pubblico e privato.



T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Cosa fare

Il criterio


Nell'eseguire i propri compiti il RPD
considera debitamente
i rischi inerenti al trattamento, tenuto conto
della natura
dell'ambito di applicazione
del contesto
delle finalità del medesimo.

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Come fare a stabilire delle priorità?

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Definire delle policy e farle conoscere!

- La gestione dei diritti degli interessati
- I data breach
- Le richieste istruttorie dell'Autorità
- La formazione degli atti

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Il piano della formazione

Risorse umane

Gli strumenti

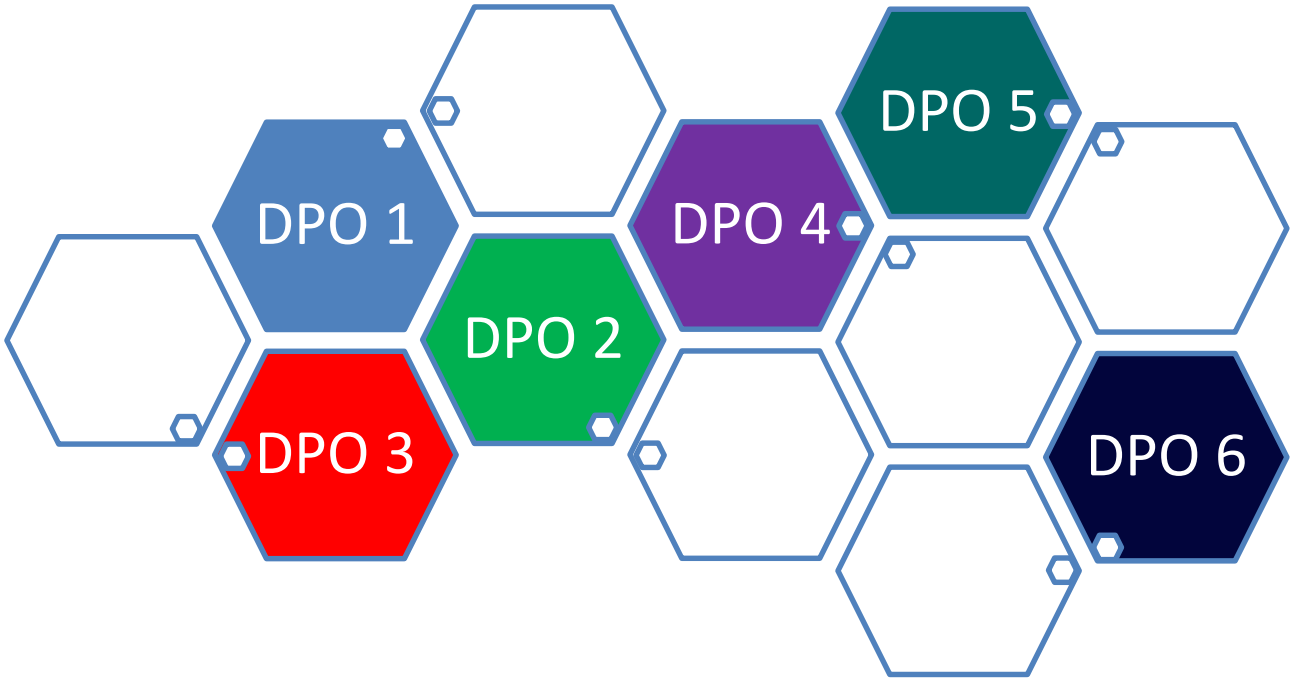
Quali livelli

Sensibilizzazione e formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Fare rete!

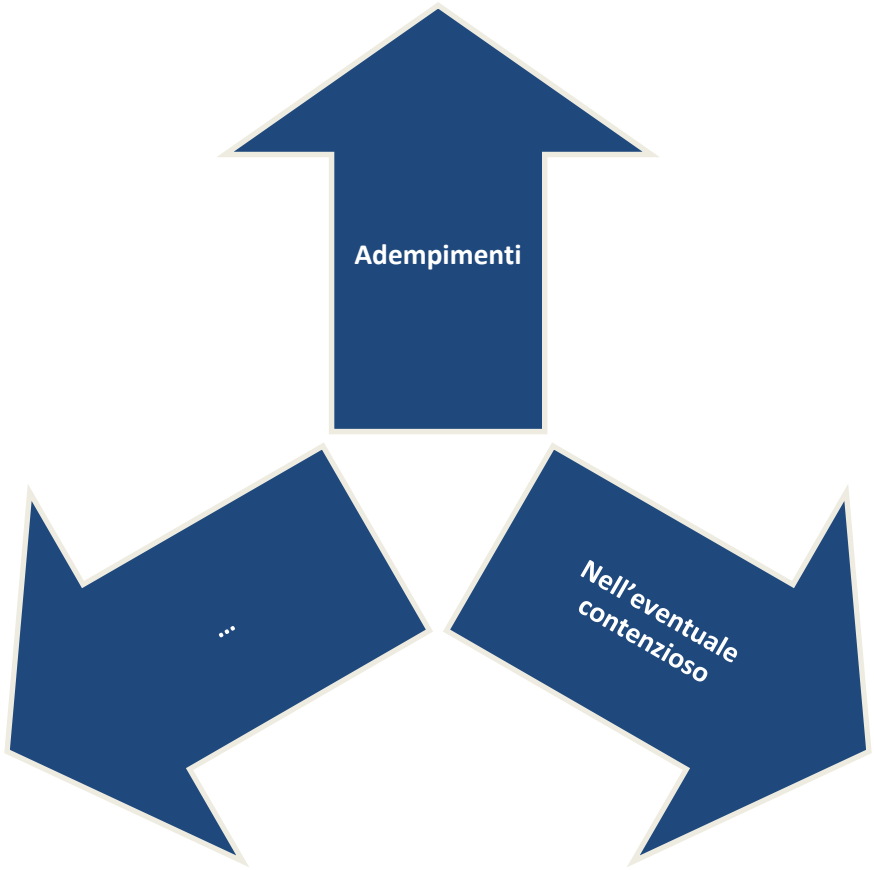


T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Cosa NON fare

Sostituirsi al titolare/responsabile



T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Mai dimenticarsi di avere un ruolo di garanzia

L'autorità di controllo e i RPD danno vita ad un "partenariato strategico"

→

le DPA incoraggiano gli interessati (in primo luogo e soprattutto) a risolvere eventuali problemi direttamente con i RPD

↓

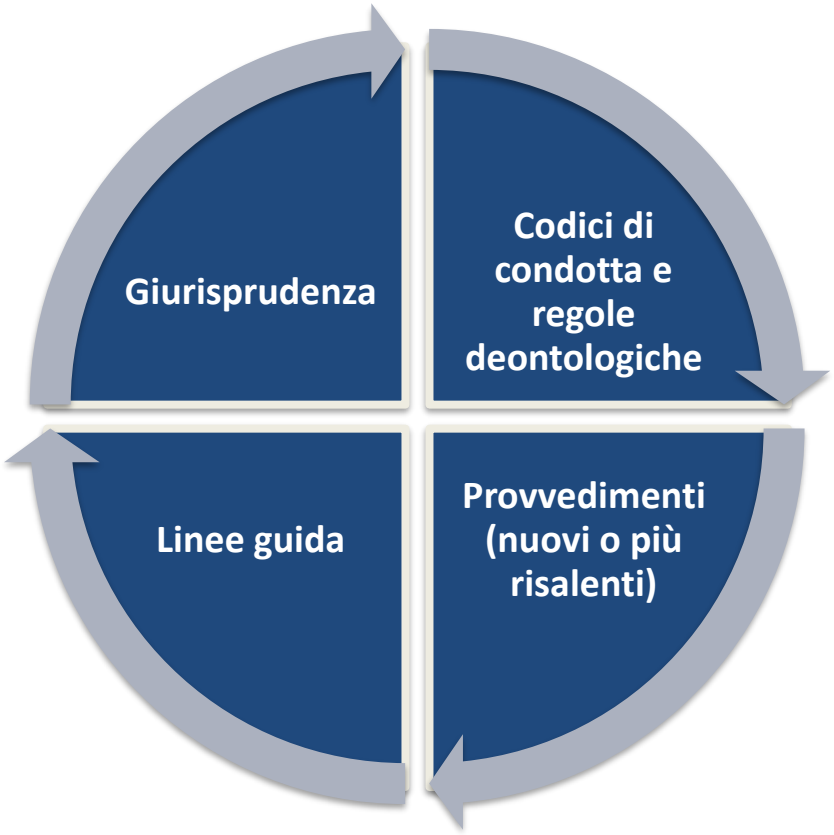
i RPD devono essere in grado – ed hanno il compito – di collaborare con l'Autorità per garantire che le risposte alle domande e ai reclami siano gestite in modo corretto e producano, se del caso, i cambiamenti necessari nelle prassi del titolare

→

Le DPA devono poter fare affidamento sui RPD e sulla loro capacità di essere al fianco degli interessati per qualsiasi reclamo.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Evitare di far prevalere le semplici opinioni ai fatti



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4DATA

In collaborazione con REGIONE MARCHE

EVENTO FORMATIVO SUL RGPD

REGOLAMENTO (UE) 2016/679

Il trattamento dei dati personali per finalità di cura e ricerca

Regole deontologiche, codici di condotta e misure di garanzia

Silvia Melchionna
Dipartimento sanità e ricerca

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Ancona, 7 giugno 2019

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

Regole deontologiche, codici di condotta e misure di garanzia

Silvia Melchionna

T4DATA

Regole deontologiche, codici di condotta e misure di garanzia

Disciplina di riferimento

Art. 9, par 4 del Regolamento – Ulteriori condizioni per i dati sulla salute

PER I DATI RELATIVI ALLA SALUTE

↓

ULTERIORI CONDIZIONI

↓

LIMITAZIONI

Art. 9, par 4 del Regolamento – Ulteriori condizioni per i dati sulla salute

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CONDIZIONI DI LICEITÀ IN AMBITO SANITARIO

Art. 9 RGPD

Art. 75 e ss. del Codice

Art. *2-septies* del Codice

Specifiche disposizioni di settore

TRATTAMENTI PER FINI DI CURA

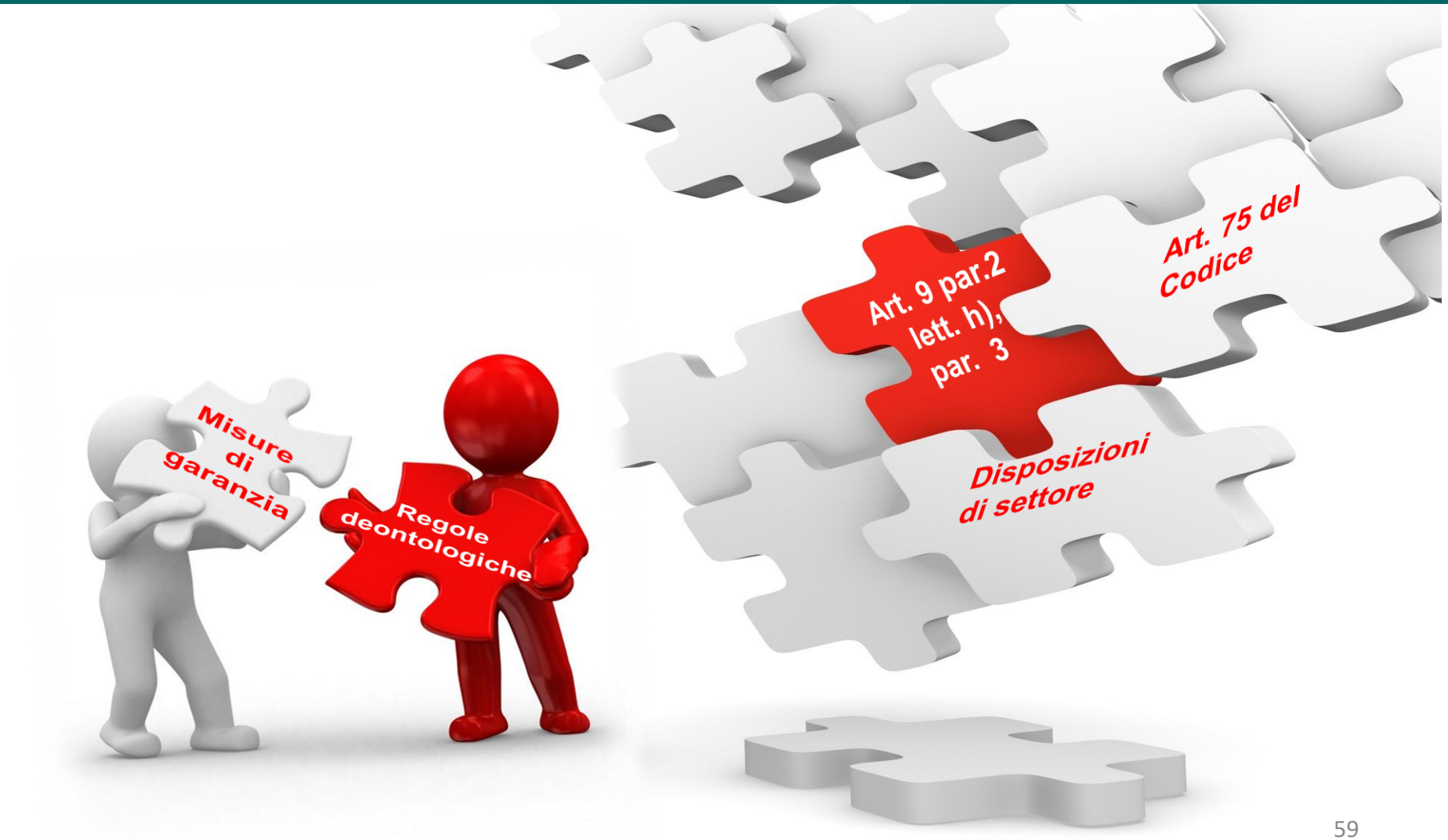
…a completare il quadro regolatorio

REGOLE DEONTOLOGICHE

(art. 2 quater Codice)

Per i trattamenti di dati relativi alla salute per finalità di cura

Condizioni di liceità dei trattamenti per fini di cura



MISURE DI GARANZIA

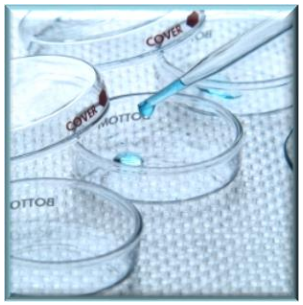
ART. 2 SEPTIES

Disposte dal Garante

DATI SULLA SALUTE

Conformità alle misure

MISURE DI GARANZIA



DATI GENETICI
BIOMETRICI E SALUTE

COMITATO EUROPEO
EVOLUZIONE SCIENTIFICA
LIBERA CIRCOLAZIONE

REVISIONE BIENNALE
CONSULTAZIONE PUBBLICA

MISURE DI GARANZIA

CONTRASSEGNI ZTL
GESTIONE SANITARIA
COMUNICAZIONE DIAGNOSI
PRESCRIZIONI

PER CIASCUNA CATEGORIA DI DATI:
salute, genetici e biometrici

SPECIFICHE FINALITA'

MISURE DI GARANZIA

INDIVIDUANO

- **ULTERIORI CONDIZIONI DI LICEITÀ**
  - Per dati genetici se rischio elevato
    - **Consenso interessato**
- **MISURE DI SICUREZZA**
  - Tecniche di cifratura pseudonomizzazione
- **MINIMIZZAZIONE**
- **MODALITÀ ACCESSO SELETTIVO e per rendere INFORMAZIONI**
- **MISURE A GARANZIA DEI DIRITTI**

MISURE DI GARANZIA

IL GARANTE

- DATI GENETICI E SULLA SALUTE PER FINI DI CURA
- ORGANIZZATIVI E GESTIONALI IN AMBITO SANITARIO
- COMUNICAZIONE DIAGNOSI
- PRESCRIZIONE MEDICINALI
- SENTITO MIN. SALUTE e PARERE CONSIGLIO SUPERIORE DI SANITÀ

LIMITAZIONE

DIVIETO DI DIFFUSIONE

ART. 2 *SEPTIES*

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

REGOLE DEONTOLOGICHE

ART. 2 *QUATER* CODICE

IL GARANTE

PROMUOVE
Principio Rappresentatività

TIENE CONTO
Raccomandazioni Consiglio d'Europa

VERIFICA
conformità

ESAMINA
osservazioni

GARANTISCE
diffusione e rispetto

REGOLE DEONTOLOGICHE

- Consultazione pubblica
- Approvazione Garante
- Pubblicate su GU allegate al Codice
- Condizione di liceità e correttezza

Art. 2 *quater* del Codice

REGOLE DEONTOLOGICHE

ART 20 D.LGS N. 101/18
PROVV. 19/12/2018

Codici di deontologia e di buona condotta per i trattamenti di dati personali per scopi scientifici e statistici

Conformità al RGPD

Le disposizioni compatibili ridenominate Regole Deontologiche

REGOLE DEONTOLOGICHE PER TRATTAMENTI A FINI STATISTICI O DI RICERCA SCIENTIFICA EFFETTUATI ANCHE NELL'AMBITO DEL SISTAN

REGOLE DEONTOLOGICHE

IL GARANTE

ADOTTATO
Regole deontologiche per fini statistici e scientifici

PROMUOVERE
la Revisione

SEGUENDO
la procedura art. 2 *quater*

Art. 20 d.lgs n. 101/2018 - art. 2 quater

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Ulteriore completamento

LINEE GUIDA COMITATO EUROPEO

CODICI DI CONDOTTA

«Gli Stati membri, le autorità di controllo, il Comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese »

(art. 40 RGPD – Cons. nn. 98/99)

CODICI DI CONDOTTA

Art. 40 RGPD – Cons. 99

Associazioni organismi rappresentanti dei titolari o responsabili

ELABORARE

- Consultando le parti e gli interessati
- Tenendo conto osservazioni e opinioni

al fine di **PRECISARE** l'applicazione del RGPD

CODICI DI CONDOTTA

CODICI DI CONDOTTA

CODICI DI CONDOTTA - Linee guida europee

LINEE GUIDA IN MATERIA DI CODICI DI CONDOTTA

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CODICI DI CONDOTTA - Linee guida europee

- Utile per dimostrare *compliance* al RGPD
- Strumento di *accauntability*
- Supporto a titolari per specifici trattamenti
- *Best practies*
- Strumento di fiducia per interessati

CODICI DI CONDOTTA - Linee guida europee

- ✓ FINALITÀ E SCOPO
- ✓ COME FACILITERÀ L'APPLICAZIONE DEL RGPD
- ✓ REQUISITO DELLA RAPPRESENTATIVITÀ
- ✓ OPERAZIONI DI TRATTAMENTO COPERTE
- ✓ AMBITO NAZIONALE O TRANSFRONTALIERO
- ✓ MECCANISMI DI MONITORAGGIO DELLA COMPLIANCE AL CODICE
- ✓ NEL SETTORE PUBBLICO MECCANISMI INTERNI DI CONTROLLO
- ✓ CONSULTAZIONE CON *STAKEHOLDERS* E INTERESSATI
- ✓ RISPETTO NORMATIVE APPLICABILI NEL SETTORE

CODICI DI CONDOTTA - Linee guida europee

dimostrare che

- ✓ soddisfa particolari esigenze del settore
- ✓ facilita applicazione del GDPR
- ✓ fornisce garanzie sufficienti
- ✓ tiene conto pareri Autorità
- ✓ fornisce meccanismi efficaci per monitorare la conformità

Non deve

ripresentare i contenuti del RGPD

CODICI DI CONDOTTA - Linee guida europee

EVALUATION

SOTTOMISSIONE

Soddisfano i criteri di approvazione	Richiesta integrazione

ACCETTAZIONE

Parere positivo	Parere negativo

APPROVAZIONE

Ampia conoscibilità

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CODICI DI CONDOTTA IN AMBITO SANITARIO

ESERCIZIO DIRITTI

APPARECCHIATURE ELETTROMEDICALI

TEMPI DI CONSERVAZIONE DOCUMENTAZIONE SANITARIA

STRUTTURE SANITARIE

Codici di condotta e regole deontologiche

ORGANISMI RAPPRESENTATIVI

GARANTE

CODICI DI CONDOTTA

REGOLE DEONTOLOGICHE

DIFFERENZE

REGOLE DEONTOLOGICHE
(art. 2 quater del Codice)

- Garante **promuove**
- Art. 9, par. 4 e altro
- Condizione di correttezza e liceità
- Verifica del Garante consultazione pubblica e Allegate al Codice

CODICI CONDOTTA
(art. 40 RGPD)

- Garante **incoraggia**
- Vari settori
- Elemento di *accauntability*
- Emanato da rappresentanti e parere del Garante
- Diffusione

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4DATA

In collaborazione con REGIONE MARCHE

EVENTO FORMATIVO SUL RGPD

REGOLAMENTO (UE) 2016/679

Il trattamento dei dati personali per finalità di cura e ricerca

Presupposti di liceità del trattamento in ambito sanitario: il consenso e l'interesse pubblico

Francesca Cecamore
Dipartimento sanità e ricerca

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Ancona, 7 giugno 2019

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

Presupposti di liceità del trattamento in ambito sanitario: il consenso e l'interesse pubblico

Francesca Cecamore

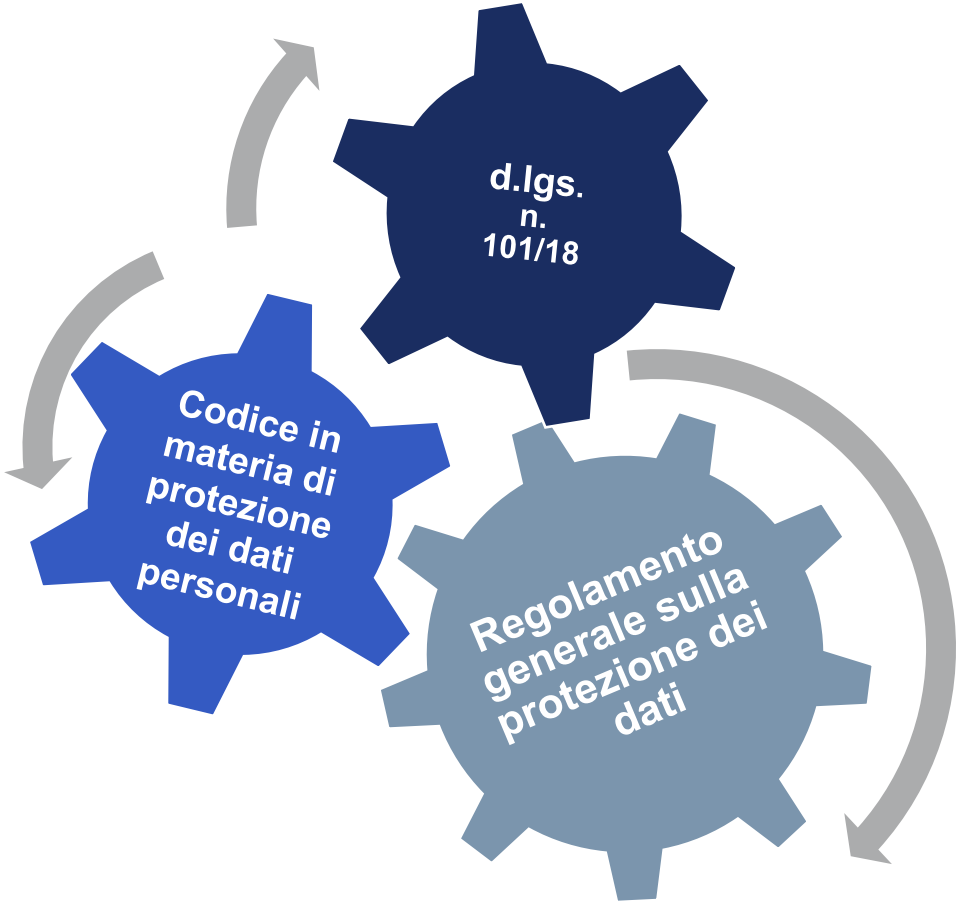
T4DATA

Presupposti di liceità del trattamento in ambito sanitario: il consenso e l'interesse pubblico

Di cosa parleremo

1. **Quadro giuridico di riferimento: disposizioni applicabili e definizione dei dati sulla salute**
2. **Trattamento dei dati sulla salute in ambito sanitario per finalità di cura**
3. **Trattamento dei dati sulla salute in ambito sanitario per motivi di interesse pubblico rilevante**
4. **Informazioni da fornire agli interessati**

Framework normativo di riferimento



Definizione dati sulla salute

Art. 4 (15):	• Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute
Considerando n. 35	• Tutti i dati che rivelano info sulla salute presente, passata o futura. Sono ricomprese un numero, un simbolo o un elemento specifico attribuito a una persona fisica, qualsiasi informazione relativa a malattie, disabilità, anamnesi medica, trattamenti clinici



In particolare, per i trattamenti in ambito sanitario il quadro di riferimento

Art. 9 del Regolamento

Artt. *2-sexies*, *2-septies* e 75 e ss. del Codice

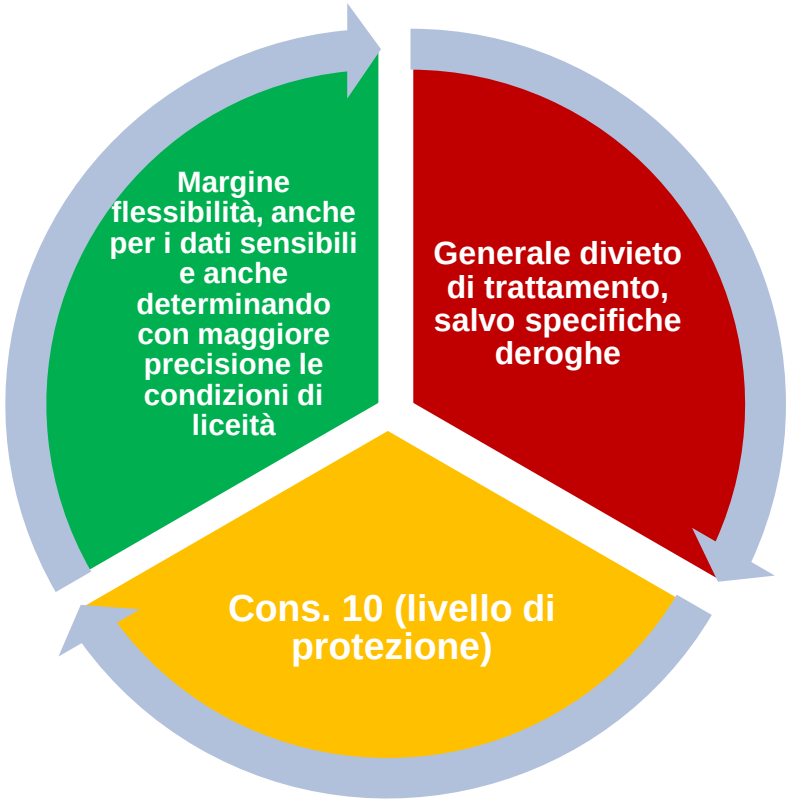
Specifiche disposizioni di settore

Fase transitoria (artt. 20 e 21 del d. lgs. n. 101/2018)

- Aggiornamento delle autorizzazioni generali e individuazione delle prescrizioni considerate compatibili e sottoposte a consultazione pubblica (Provv. 13 dicembre 2018)
- Cessazione effetti autorizzazione n. 2 sulla salute
- Verifica della conformità dei codici deontologici e conversione in regole deontologiche (Provv. 19 dicembre 2018)

Il sistema è in fase di definizione

Art. 9, par 1 Regolamento – divieto di trattamento di particolari categorie di dati



Art. 9, par 2: le deroghe al divieto di trattamento delle particolari categorie di dati applicabili al settore sanitario

Il trattamento è necessario **per motivi di interesse pubblico** rilevante, sulla base del diritto europeo o nazionale, che deve essere **proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato** (art. 9, par. 2, lett. g; C55 e C56)

Il trattamento è necessario per **motivi di interesse pubblico nel settore della sanità pubblica** (es. protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici) (art. 9, par. 2, lett. i); C54)

Il trattamento è necessario per perseguire finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, **diagnosi, assistenza o terapia sanitaria o sociale** ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, se i dati sono trattati da o **sotto la responsabilità di un professionista soggetto al segreto professionale** (art. 9, par. 2, lett. h) e par. 3; C.53)

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Art. 9, par 2: le deroghe al divieto di trattamento delle particolari categorie di dati applicabili al settore sanitario

Numerosi quesiti sul nuovo assetto normativo
Esigenza di chiarimenti da parte di operatori, soggetti istituzionali, DPO e cittadini
Chiarimenti dell'Autorità, pur in un quadro regolatorio incompleto

Provvedimento
7 marzo 2019
(doc. web n. 9091942)

RGPD
REGOLAMENTO (UE) 2016/679

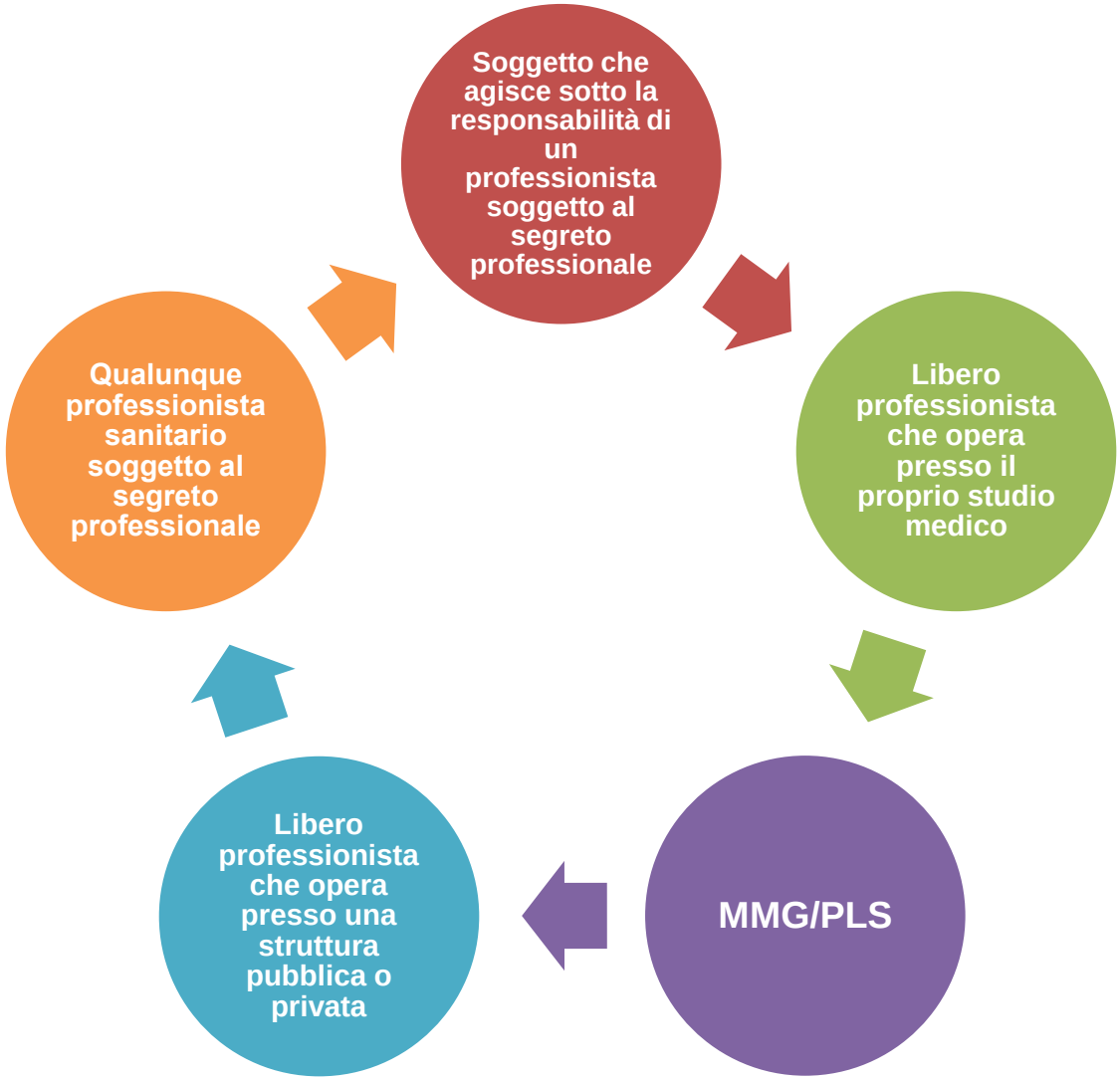
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario

Trattamenti necessari per «finalità di cura» art. 9, par. 2 lett. h) e par. 3

Deroga che si applica al coesistere di due condizioni

Art. 9, par. 3: soggetti ai quali si applica la deroga

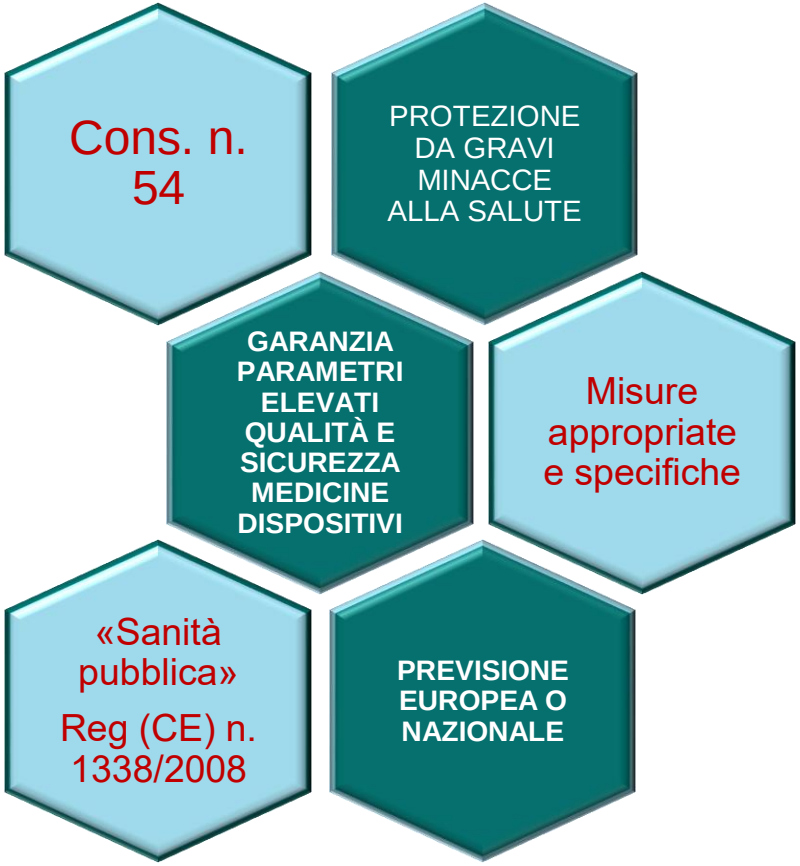


Particolari casi di trattamento

CONSENSO

- *App* mediche
- Fidelizzazione clientela
- Finalità promozionali o commerciali
- Finalità commerciali o elettorali
- Fascicolo Sanitario Elettronico
- Referti *on-line*
- *Dossier* sanitario

Trattamenti necessari per motivi di sanità pubblica: art. 9, par. 2, lett. i)



Trattamenti necessari per motivi di interesse pubblico rilevante: art. 9, par. 2, lett. g)

il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto europeo o nazionale, a prescindere dalla natura soggettiva di coloro che effettuano il trattamento (soggetti pubblici e privati) e che deve essere

Trattamenti necessari per motivi di interesse pubblico rilevante: art. 9, par. 2, lett. g)

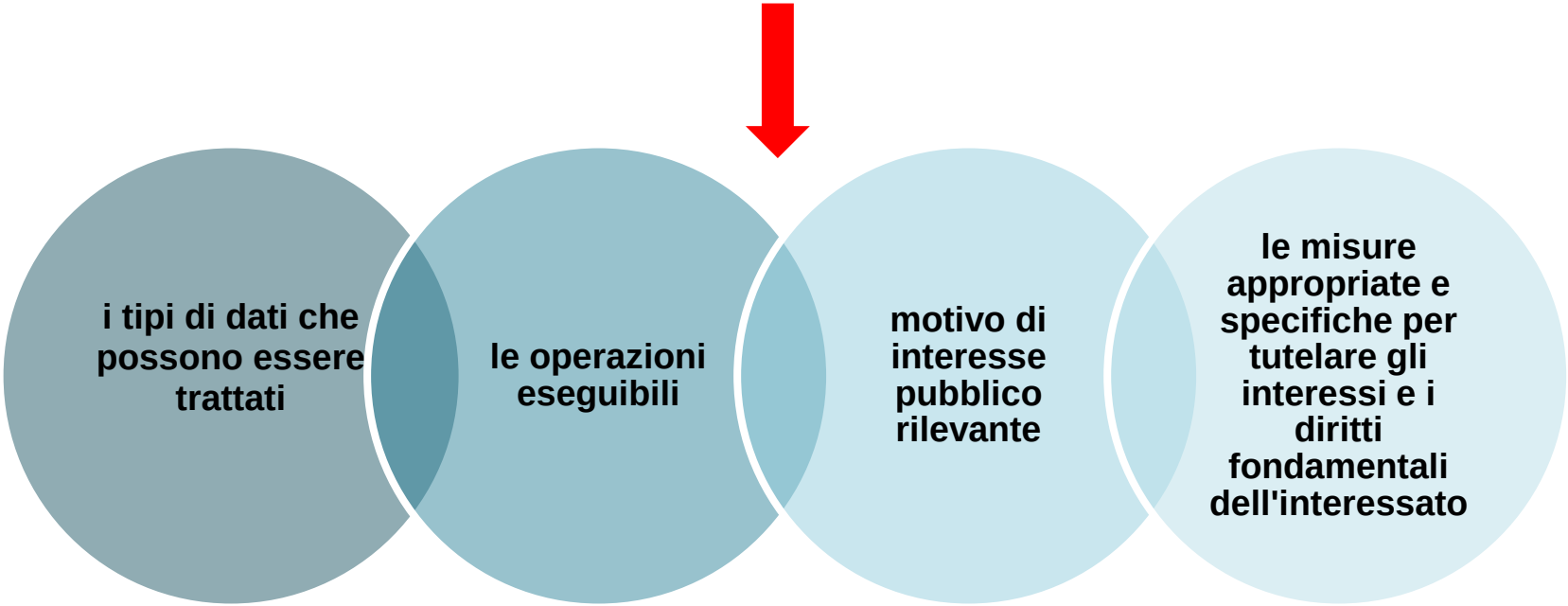
Principio di proporzionalità

Imposizione di oneri non sproporzionati rispetto ai fini perseguiti e scelta della misura meno restrittiva dei diritti che si fronteggiano

Previsione, in ogni caso, di misure per la minor lesione possibile del diritto alla protezione dei dati personali

Disposizione attuativa: art. *2-sexies* del Codice

I trattamenti dei dati sulla salute necessari per motivi di interesse pubblico rilevante (art. 9 paragrafo 2, lettera g)) sono ammessi se previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino:



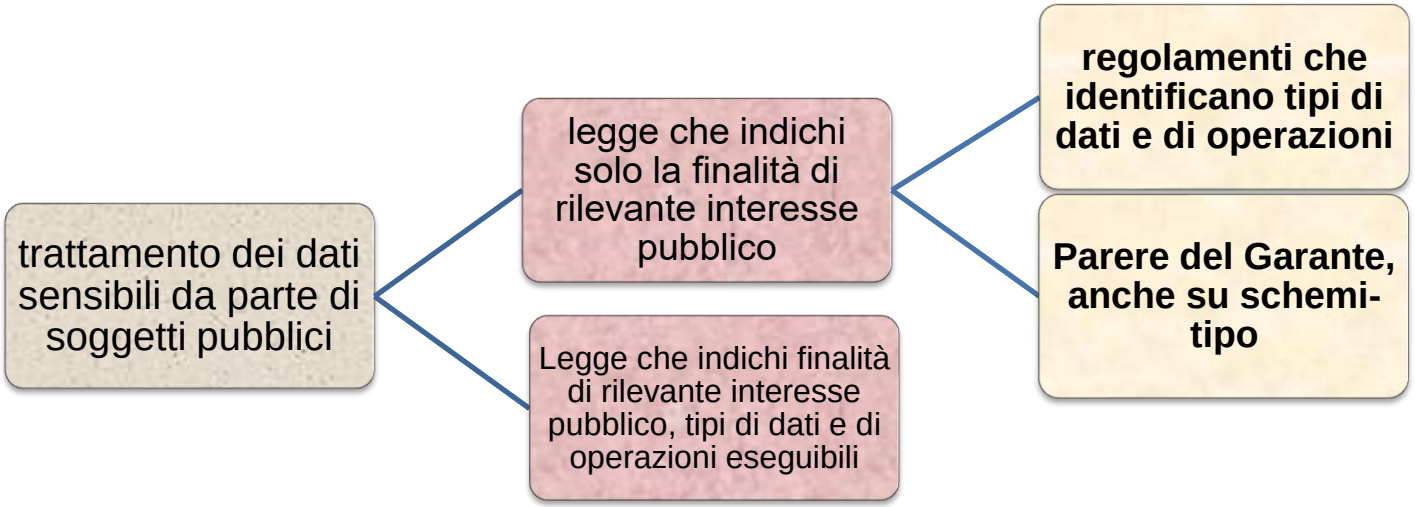
Trattamenti per motivi di interesse pubblico rilevante in ambito sanitario

Soggetti con compiti di interesse pubblico o connessi all'esercizio di pubblici poteri: art. *2-sexies*, comma 2, del Codice

- Attività amministrative e certificatorie correlate alla cura (lett. t))
- Compiti del SSN (lett. u))
- Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria (lett. v))
- Vigilanza sulle sperimentazioni, farmacovigilanza (lett. z))
- Tutela della maternità e IVG, dipendenze, assistenza, integrazione sociale e diritti disabili (lett. aa))

Trattamenti per motivi di interesse pubblico rilevante in ambito sanitario

Facciamo un passo indietro: art. 20 del Codice pre-decreto n. 101/2018



Trattamenti per motivi di interesse pubblico rilevante in ambito sanitario

Schema-tipo regolamento dati sensibili ASL

Trattamenti per motivi di interesse pubblico rilevante in ambito sanitario

Schema-tipo regolamento dati sensibili ASL

Informazioni da fornire all'interessato (artt. 13 e 14 del Regolamento)

Informazioni da fornire all'interessato: nuovi elementi

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4DATA

In collaborazione con REGIONE MARCHE

EVENTO FORMATIVO SUL RGPD

REGOLAMENTO (UE) 2016/679

Il trattamento dei dati personali per finalità di cura e ricerca

La ricerca scientifica, medica biomedica ed epidemiologica

Chiara di Somma
Dipartimento sanità e ricerca

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Ancona, 7 giugno 2019

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Chiara di Somma

T4DATA

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Di cosa parleremo

1. **Premessa.**
2. **Condizioni di liceità del trattamento**
3. **L'art. 110 del Codice – regime previdente**
4. **L'art. 110 del Codice**
5. **Prescrizioni relative al trattamento di dati personali per scopi di ricerca scientifica**

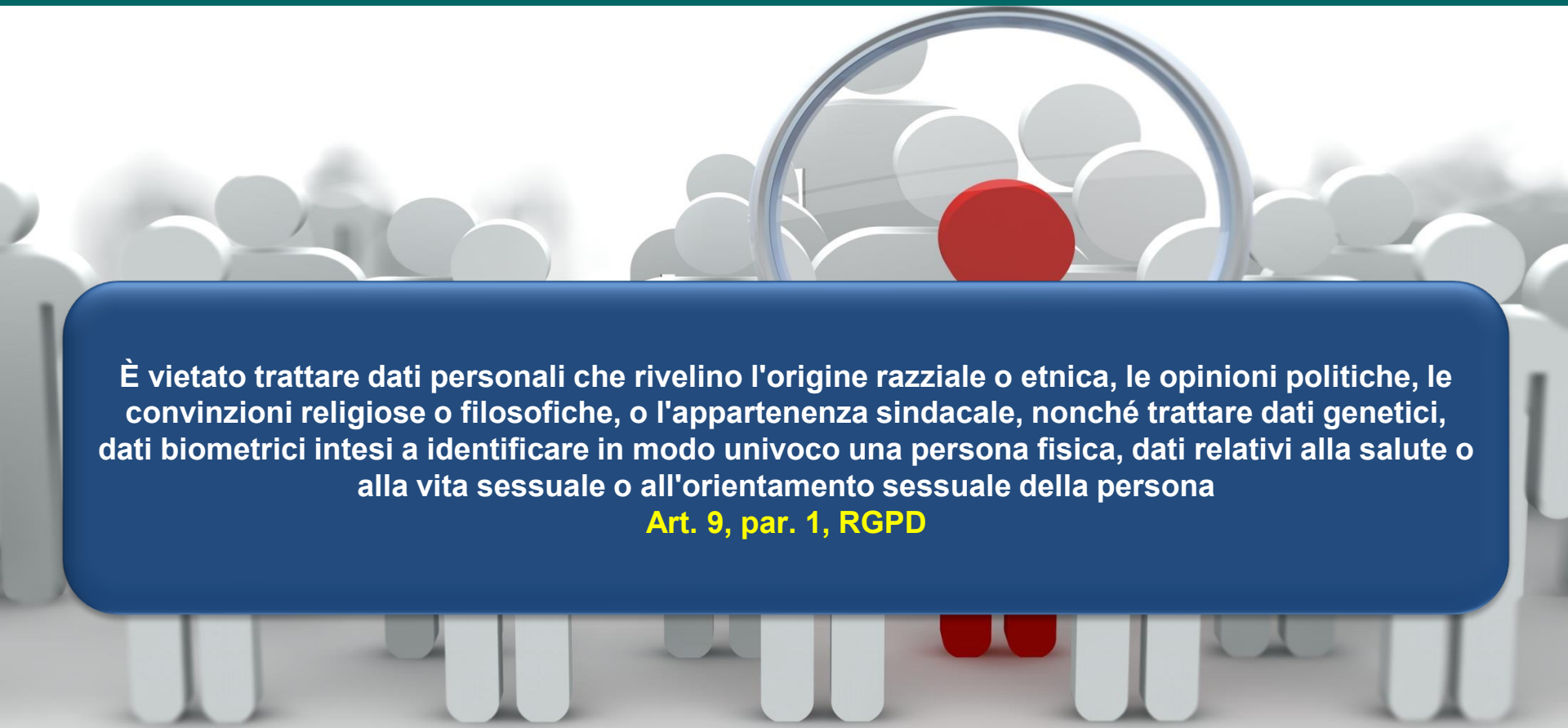
Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Premessa

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Condizioni di liceità del trattamento

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica



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

Art. 9, par. 1, RGPD

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Condizioni di liceità del trattamento

Rinvio dell'esame

Consenso → Art. 6, par. 1, lett. a), RGPD → Art. 9, par. 2, lett. a), RGPD

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Condizioni di liceità del trattamento

Art. 9, par. 2, lett. j), RGPD

Il trattamento è necessario a fini di ricerca scientifica in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che 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

L’art. 89 del Regolamento

- Garanzie adeguate
- Misure tecniche e organizzative
- Minimizzazione e pseudonimizzazione

L'art. 89 del Regolamento

Deroghe

Ai diritti di cui agli articoli da 15 a 22 RGPD

Se rischiano di rendere impossibile o pregiudicare gravemente le finalità di ricerca

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

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

Art. 9, par.4, RGPD

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Il Garante ha verificato la conformità al Regolamento delle disposizioni contenute nei codici di deontologia e di buona condotta allegati al Codice e la ha ridenominate
Regole deontologiche
Art. 20, d.lgs. 101 del 2018

Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica
19 dicembre 2018 doc. web n. 9069637

Condizione essenziale per la liceità e correttezza del trattamento

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Prescrizioni del Garante

Il Garante con provvedimento di carattere generale da porre in consultazione pubblica individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonchè al Capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento. Il provvedimento di cui al presente comma è adottato entro sessanta giorni dall'esito del procedimento di consultazione pubblica.

Art. 21, d.lgs. 101 del 2018

Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice. 13 dicembre 2018. doc. web n. 9068972

Provvedimento finale…in corso di approvazione

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Misure di garanzia
art. *2-septies* del Codice

Art. 9, par. 4, RGPD

L'art. 110 del Codice
Regime previgente

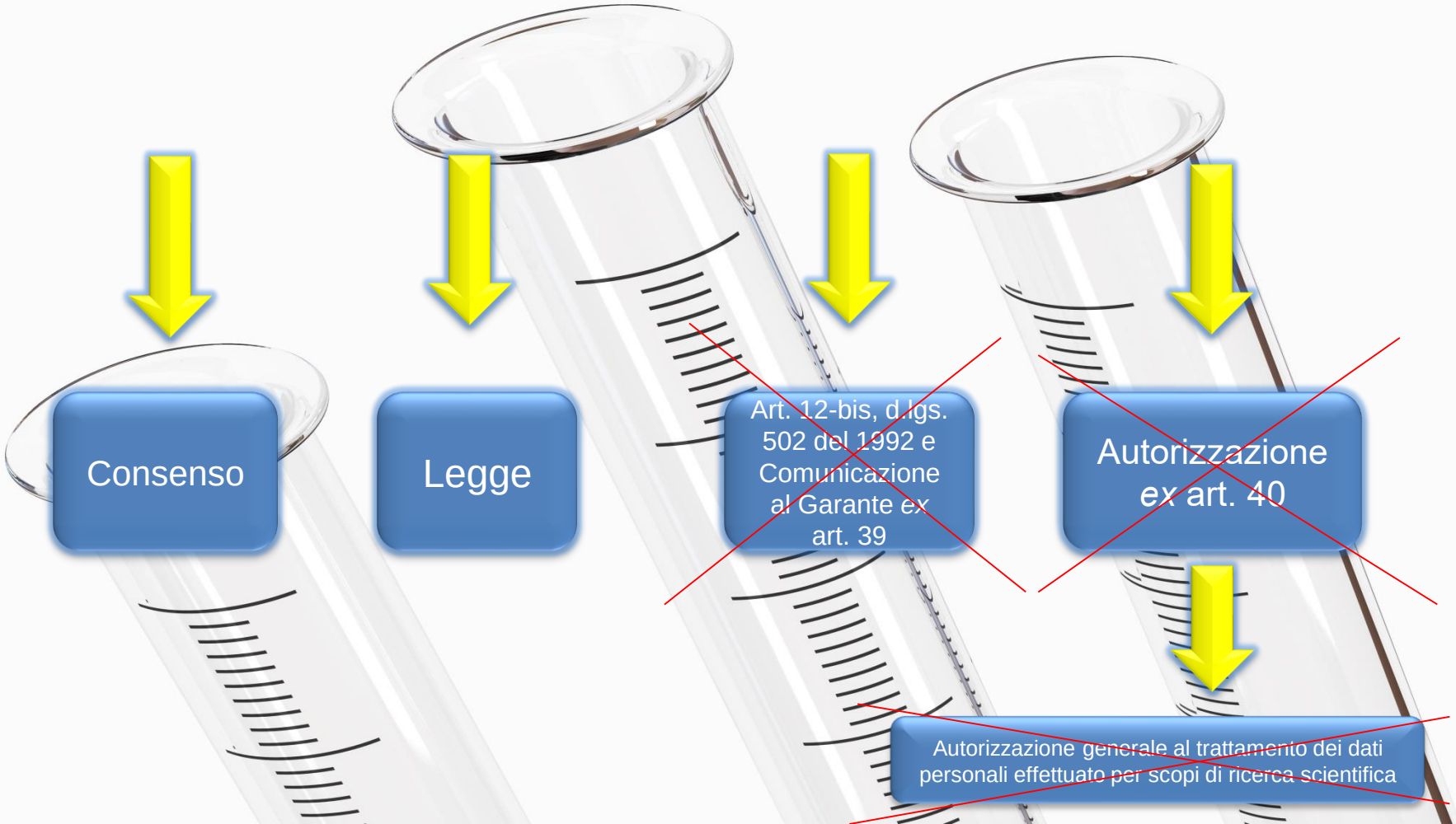
Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Il consenso dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico ed epidemiologico, non è necessario quando la ricerca è prevista da espressa disposizione di legge che prevede il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'art. 12-bis del decreto legislativo 30 dicembre 1992, n. 502, e successiva modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'art. 39. Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto del motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante ai sensi dell'art. 40

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica



Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

L'art. 110 del Codice

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. 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, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

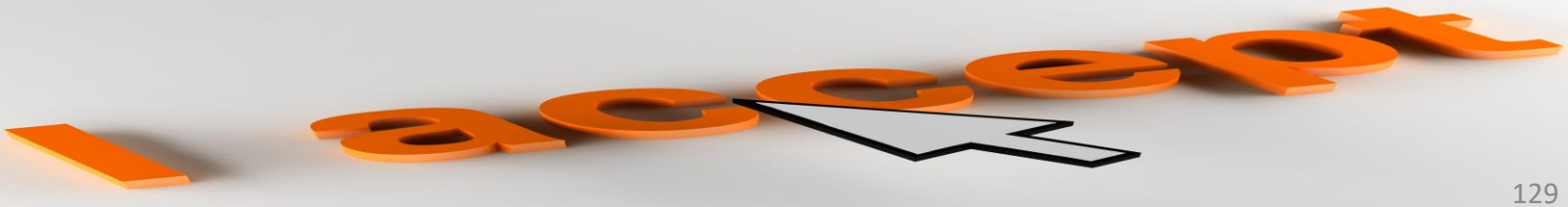
Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

consenso

Linee guida sul consenso 6/2014 Ratificate dal Board 4 aprile 2018

Parere 3/2019 del Comitato sulla sperimentazione dei medicinali

Regole Deontologiche a fini statistici o di ricerca scientifica

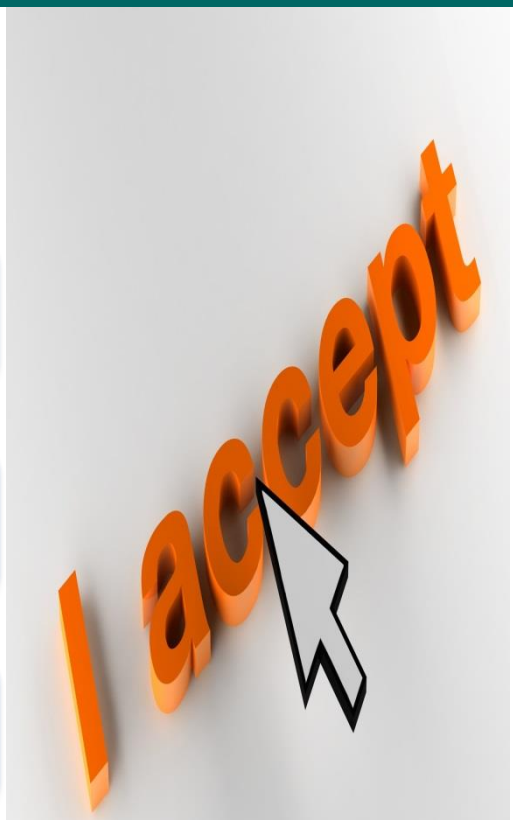


Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

L'art. 110 del Codice

Consenso esplicito

- Informato → Preceduto da idonea informativa
- Specifico → Riferito ad una determinata finalità
- Inequivocabile → Esplicito, scritto o documentato per iscritto
- Libero → Non condizionato



Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

consenso

Nel manifestare il proprio consenso l´interessato è richiesto di dichiarare se vuole conoscere o meno eventuali **scoperte inattese che emergano a suo carico durante la ricerca**. In caso positivo, i dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato (…) da parte di esercenti le **professioni sanitarie** ed organismi sanitari, solo per il tramite di un **medico designato dall'interessato** o dal titolare

Art. 8 Regole Deontologiche

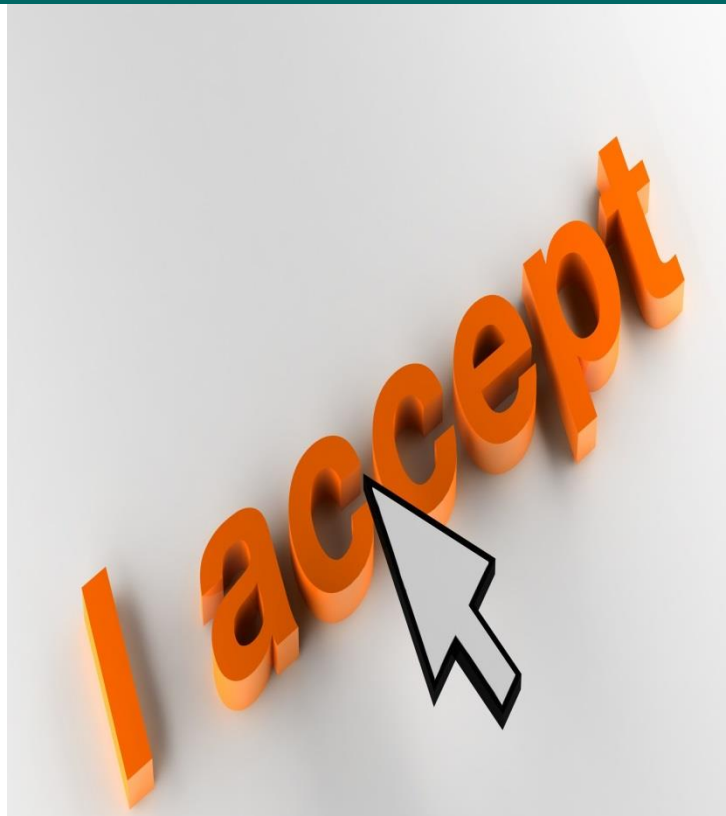
Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

consenso

Il titolare, il responsabile o le persone designate possono autorizzare per **iscritto esercenti le professioni sanitarie diversi dai medici,** che nell'esercizio dei propri compiti **intrattengono rapporti** diretti con i pazienti e sono deputati a trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai predetti soggetti.

L'atto di designazione individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati

Art. 8 Regole deontologiche



Trattamento a fini scientifica in campo medico, biomedico e epidemiologico

Trattamento a fini scientifica in campo medico, biomedico e epidemiologico

No consenso

Impossibilità di informare gli interessati

Sforzo proporzionato

Pregiudizi per la ricerca

Parere favorevole del comitato etico

Consultazione preventiva del Garante ex art. 35 e 36 RGPD

Prescrizioni relative al trattamento di dati personali per scopi di ricerca scientifica

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Ambito di applicazione

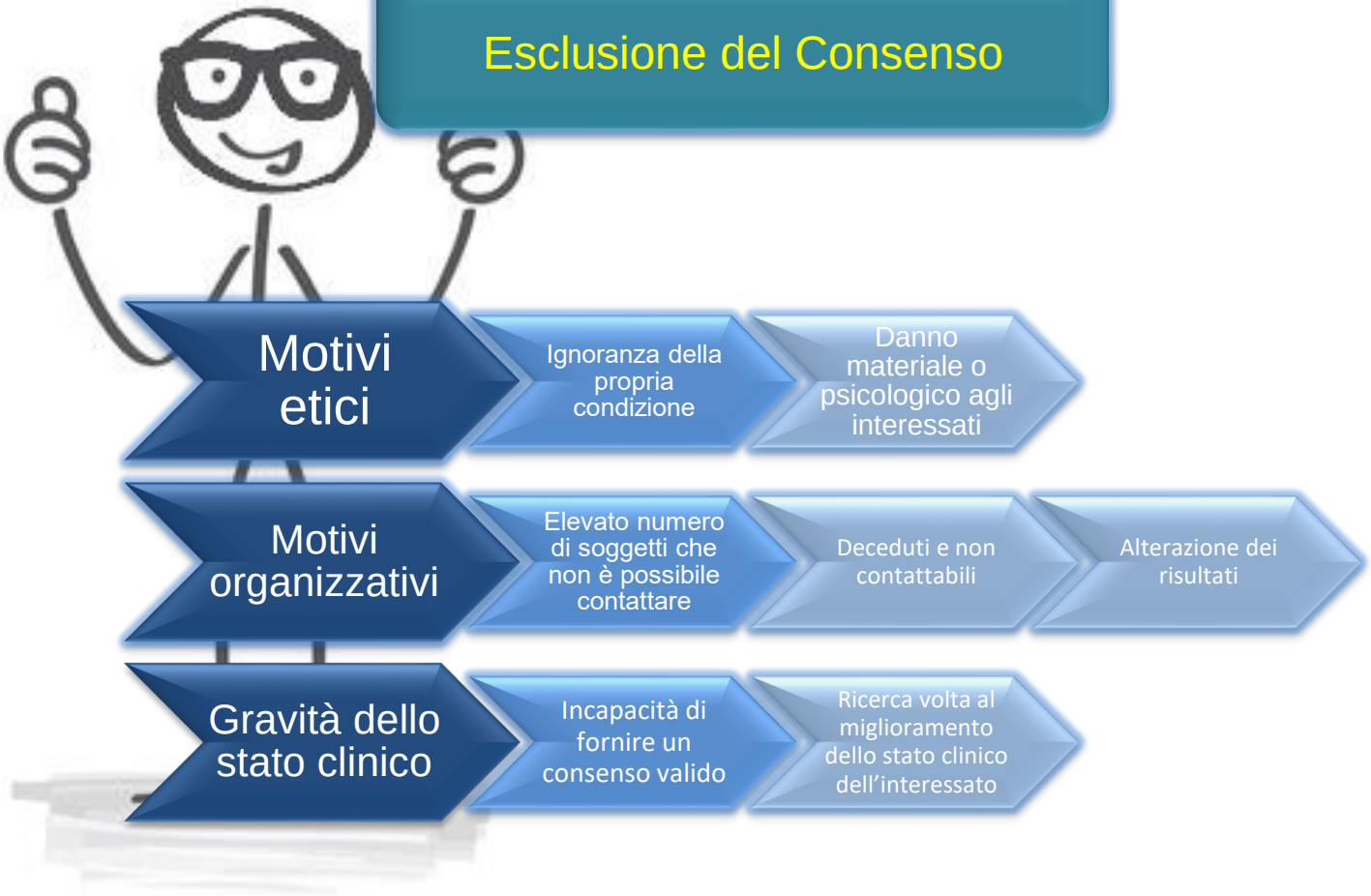
Ricerca medica, biomedica e epidemiologica ex art. 110 del Codice

a) università, altri enti o istituti di ricerca e società scientifiche, nonché ricercatori che operano nell'ambito di detti soggetti

b) esercenti le professioni sanitarie e gli organismi sanitari

c) persone fisiche o giuridiche, enti, associazioni e organismi privati, nonché soggetti specificatamente preposti al trattamento quali designati o responsabili del trattamento

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica



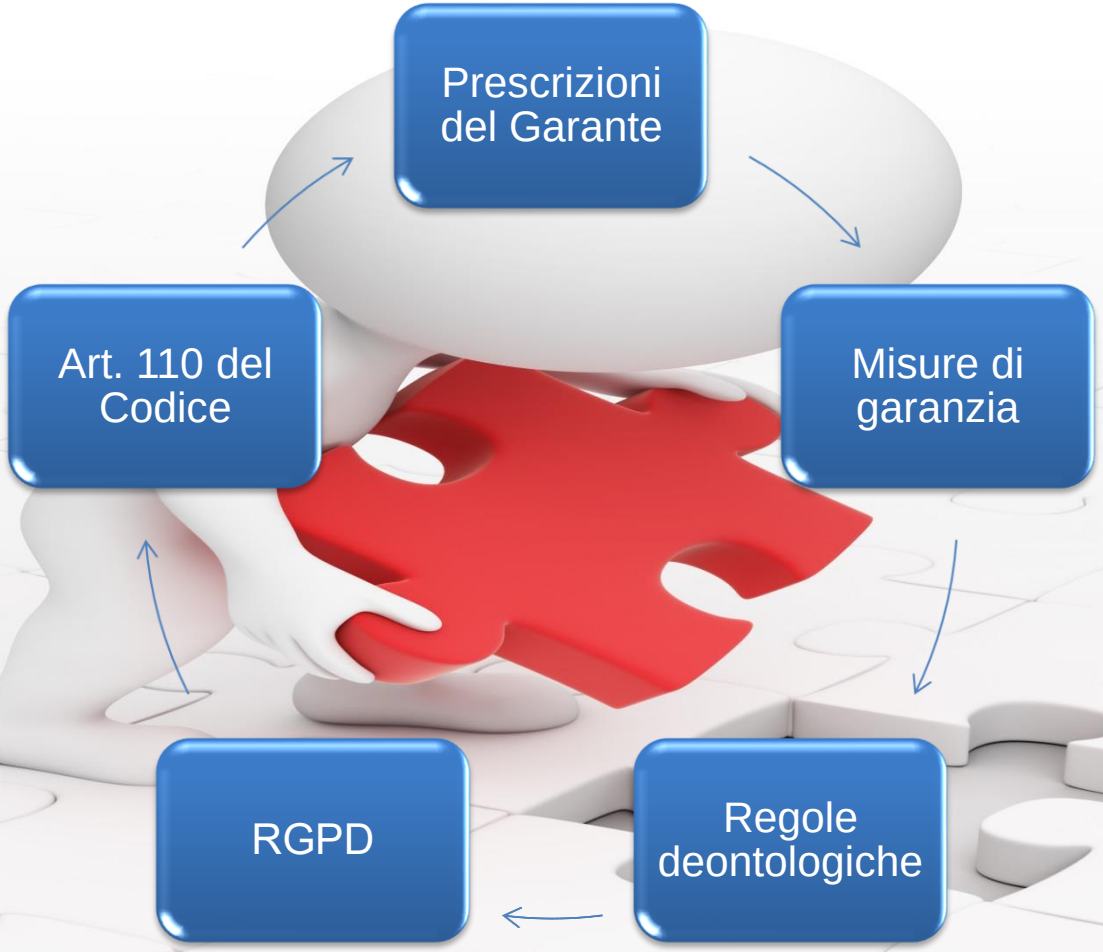
Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Minimizzazione dei dati

Il trattamento di dati personali per scopi di ricerca scientifica in campo medico, biomedico o epidemiologico può riguardare i dati idonei a rivelare lo stato di salute degli interessati e, solo ove indispensabili per il raggiungimento delle finalità della ricerca, congiuntamente anche i dati idonei a rivelare la vita sessuale e l´origine razziale ed etnica

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica

Trattamenti di dati personali per finalità di ricerca medica, biomedica e epidemiologica



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

T4DATA

In collaborazione con REGIONE MARCHE

EVENTO FORMATIVO SUL RGPD

REGOLAMENTO (UE) 2016/679

Il trattamento dei dati personali per finalità di cura e ricerca

Esame di alcuni casi pratici all'attenzione dell'Autorità relativi alla prima applicazione del RGPD

Cecilia Lugato

Dipartimento sanità e ricerca

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Ancona, 7 giugno 2019

T4DATA

Formazione delle autorità per la protezione dei dati e dei responsabili per la protezione dei dati

Esame di alcuni casi pratici all'attenzione dell'Autorità relativi alla fase di prima applicazione del RGPD

Cecilia Lugato

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Esame di alcuni casi pratici all'attenzione dell'Autorità relativi alla prima applicazione del RGPD

1. I poteri dell'Autorità di controllo
2. La cooperazione con l'Autorità
3. Focus sull'esercizio dei diritti degli interessati
4. I reclami
5. Le notifiche di violazioni di dati personali (cd *data breach*)
6. Gli ammonimenti e le sanzioni pecuniarie

L’accountability e l’attività dell’Autorità

Art. 5, par. 2 e C74

Art. 24, par. 1 e C74/78

Principio di Accountability del Titolare

L’attività del Garante interviene essenzialmente ex post
dopo le determinazioni autonome del titolare

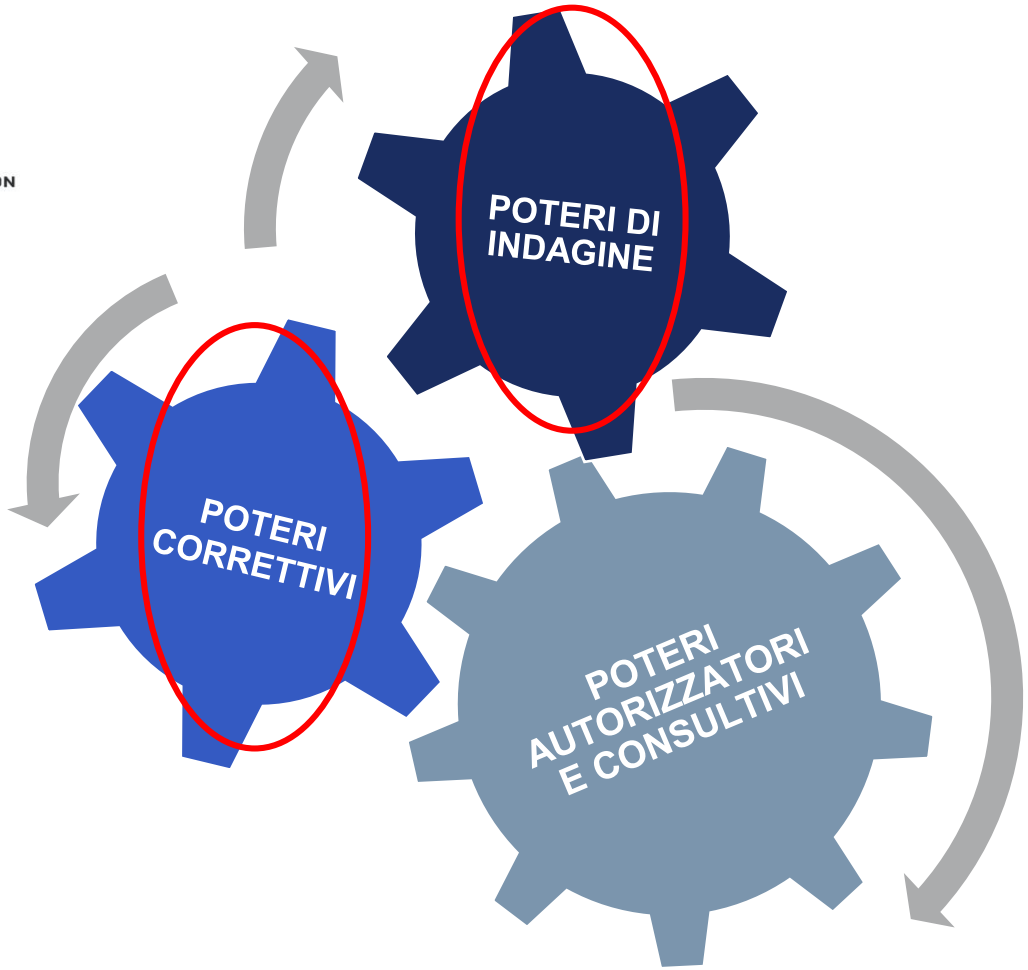
La cooperazione del titolare e del responsabile agevola lo svolgimento delle competenze dell’Autorità’

T4DATA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

I poteri dell'Autorità di controllo (art. 58 RGPD)

GDPR
GENERAL
DATA PROTECTION
REGULATION

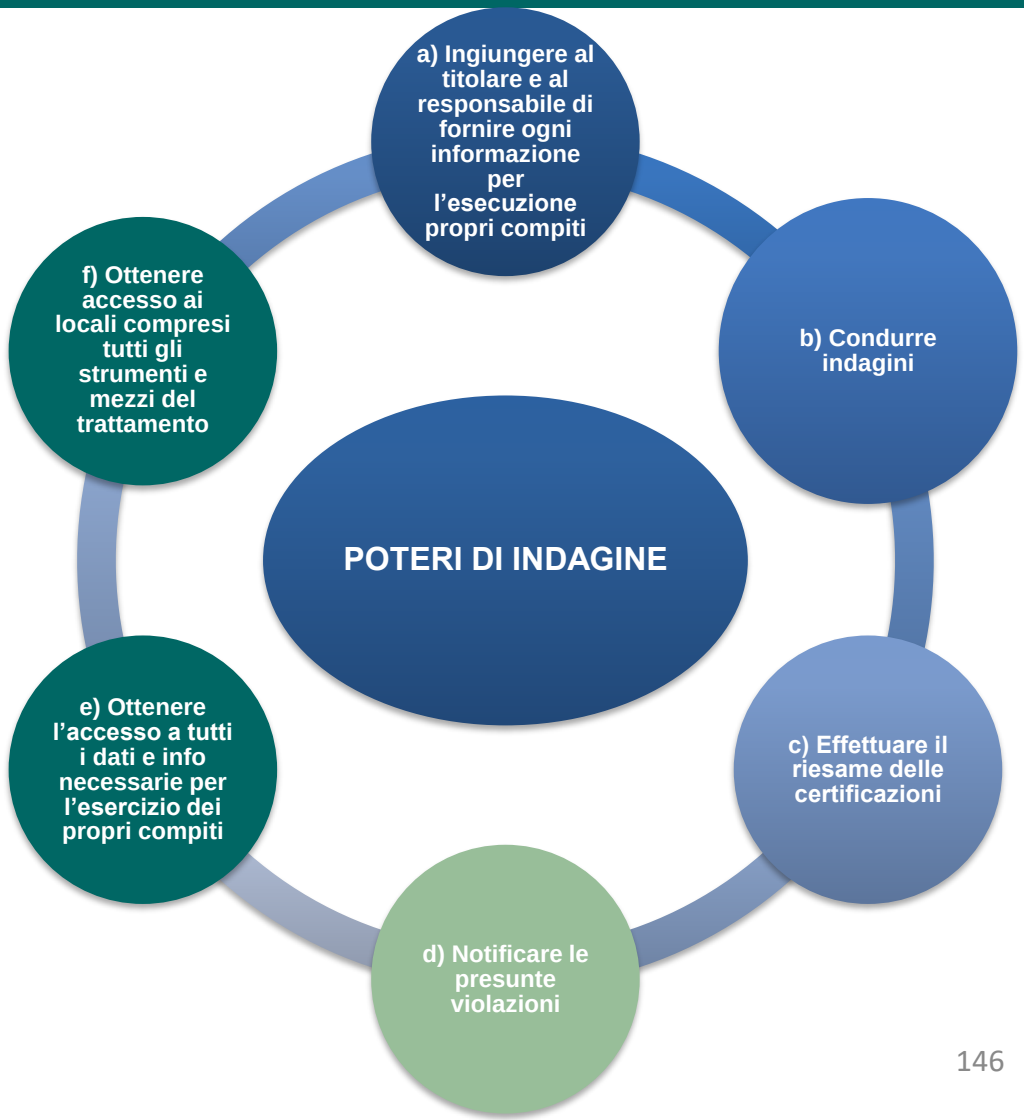


I poteri di indagine (art. 58, par 1 RGPD a 157 e 158 del Codice)

Poteri di accertamento

Poteri di accesso

Poteri che includono
Potere di imporre una limitazione provvisoria o definitiva al trattamento incluso divieto di trattamento

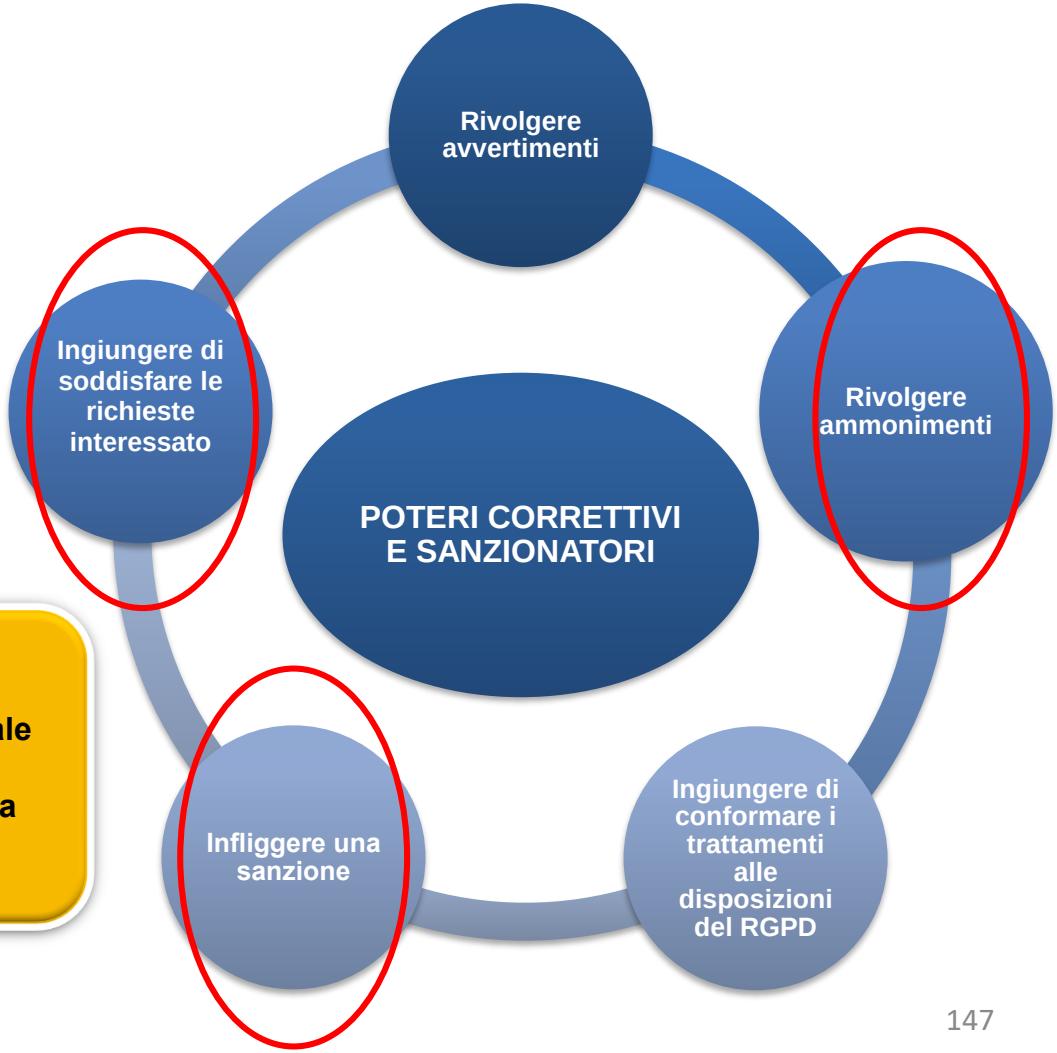


I poteri correttivi dell'Autorità (art. 58, par 2 RGPD)

Misure correttive e sanzioni pecuniarie

Poteri

1. **esercitati nel rispetto di «garanzie adeguate»: principio del contraddittorio, in modo imparziale ed equo**
2. **misura appropriata, necessaria e proporzionata tenendo conto delle circostanze di ciascun singolo caso**



Fondamentale la cooperazione con l'Autorità di controllo (art.31 RGPD)

Richiesta dall'Autorità nello svolgimento dei propri compiti e nell'esercizio dei propri poteri, espressione del principio di *accountability*

Quali sono i compiti per i quali l'Autorità può richiedere la cooperazione del Titolare/Responsabile? (art. 57 RGPD e 154 del Codice)

- **Sorveglia e assicura l'applicazione del regolamento e controlla che i trattamenti siano effettuati nel rispetto della normativa applicabile**
- **Tratta di reclami proposti dall'interessato**
- **Svolge le indagini opportune sull'oggetto del reclamo**
- **Svolge indagini sulla applicazione del Regolamento anche sulla base di info ricevute da altre Autorità (cd cooperazione)**
- **Avvia procedimento per l'applicazione delle misure correttive e delle sanzioni**
- **…….**

GDPR GENERAL DATA PROTECTION REGULATION

La cooperazione con l'Autorità di controllo perché è importante?

Art. 157 del Codice e 83, par. 5 RGPD

- Il Garante nell'esercizio dei propri compiti
- può chiedere al Titolare, al Responsabile .. di fornire informazioni e di esibire il documenti
- Altrimenti sanzione fino a 20 milioni o per le imprese fino al 4% del fatturato

Art. 83, par. 2 RGPD C148, 150 e 152

- Al momento di decidere se infliggere una sanzione amministrativa pecuniaria
- e di fissare l'ammontare della stessa in ogni singolo caso si tiene conto
- degli elementi indicati dalla lett. A) alla lett. K)

Art. 168 del Codice Privacy

- è punito con la reclusione sino ad un anno
- chiunque intenzionalmente cagiona
- un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

Cooperazione importante anche per scongiurare, in via teorica, ipotesi di reato

L’esercizio dei diritti da parte degli interessati

1. Rappresenta una delle parti più significative del Regolamento, unitamente ai principi, è un elemento primario della protezione dei dati personali
2. L’Autorità spinge affinché l’interessato si rivolga direttamente al titolare o al responsabile del trattamento e qualora non lo fa’ viene invitato a farlo
3. Tra i compiti del RPD vi è quello di essere un punto di contatto con l’interessato (i dati di contatto devono essere indicati nelle informazioni rese agli interessati – art. 13, par. 1 lett. b)
4. Un bravo RPD si attiva con procedure per risolvere i problemi rappresentati dagli interessati
5. Una delle priorità del RPD è proprio quella di organizzare l’esercizio dei diritti (processi, procedure e formazione)

Se il titolare non risponde, ovvero, la risposta non è soddisfacente
STRUMENTO DEL RECLAMO

L'istruttoria dell'Autorità sui Reclami aventi ad oggetto la violazione degli art. da 15 a 22 del RGDP

Art. 77 e RGPD

L'INTERESSATO che ritenga che il trattamento che lo riguarda violi il RGPD ha il diritto di proporre un reclamo all'Autorità

Unico strumento di tutela amministrativa a disposizione degli interessati in aggiunta ai rimedi giurisdizionali

Art. 142 del Codice

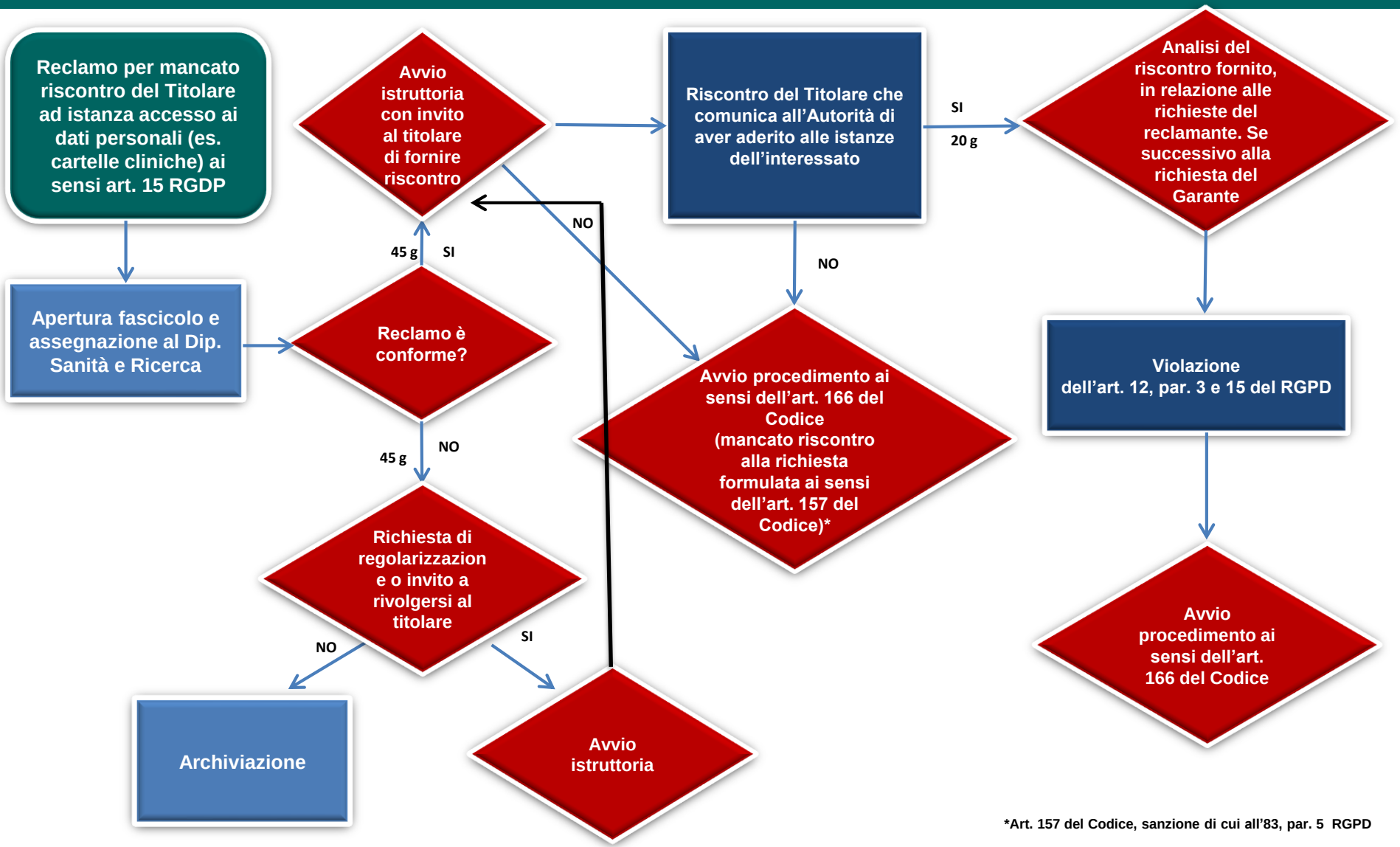
Il reclamo contiene:

1. Indicazione dettagliata dei fatti e circostanza su cui si fonda
2. Disposizioni violate
3. Misure richieste
4. Estremi identificativi del titolare e del responsabile
5. E' sottoscritto dall'interessato o avvocato o ente attivo nel settore protezione dei dati (es. associazioni dei consumatori)
6. Disponibile modello predisposto dall'Autorità

T4DATA

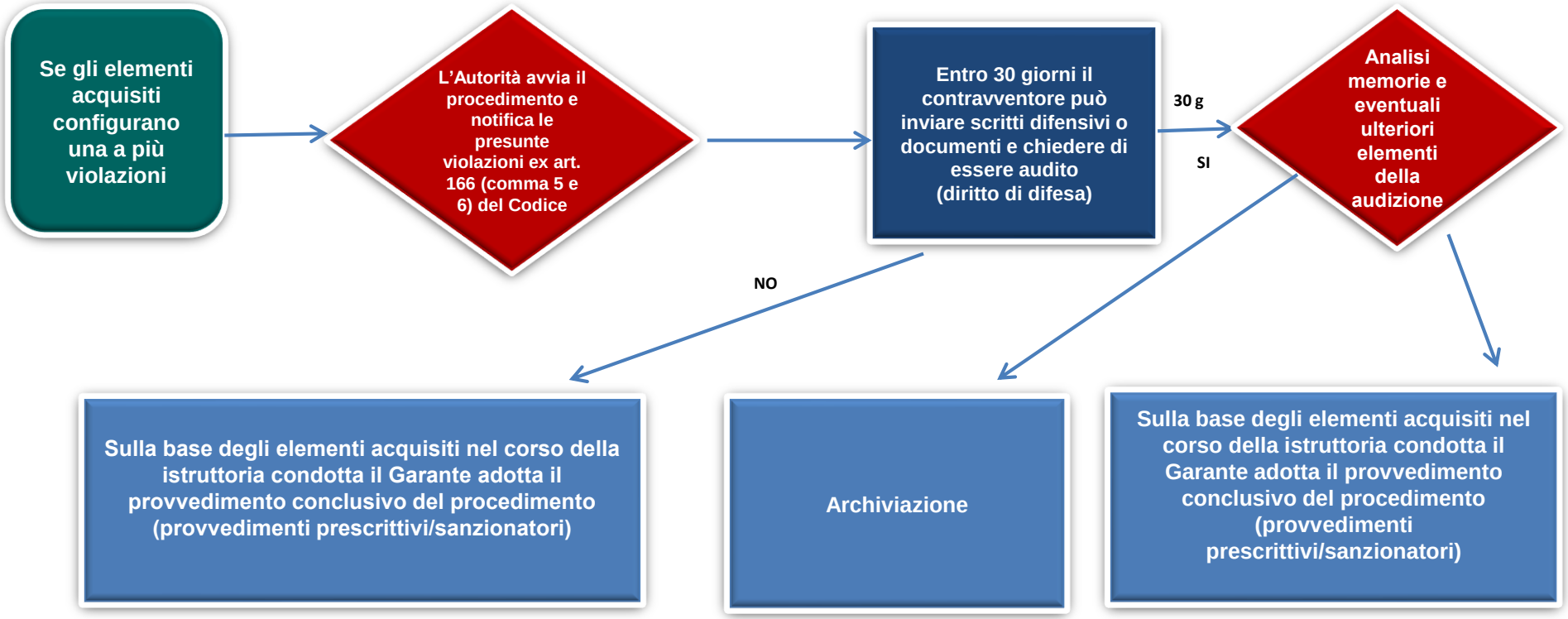
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Le istruttorie dell'Autorità sui Reclami: flow chart



*Art. 157 del Codice, sanzione di cui all'83, par. 5 RGPD

Procedimento ex art. 166 del Codice (art. 15 RGPD): flow chart

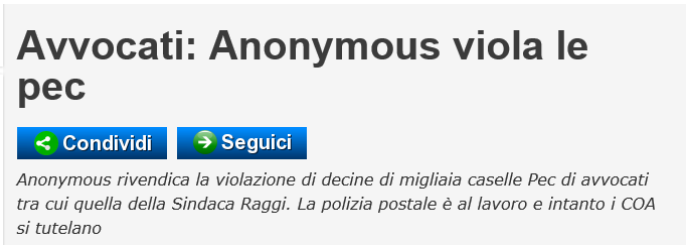


GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

La notifica di una violazioni di dati personali (cd Data Breach)

Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati
(art. 4 12) RGPD)

Dati riferiti al periodo 25 maggio 2018 - 31 marzo 2019

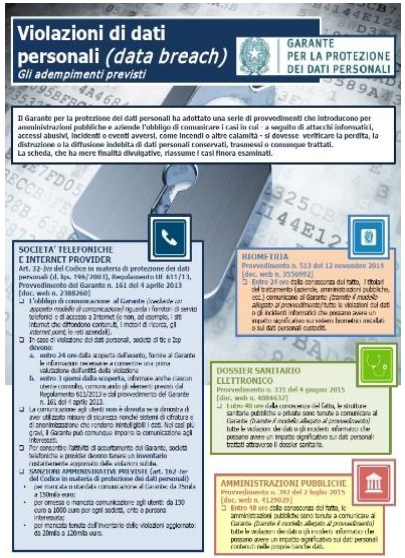


1. Aumentate in modo significativo
2. Non solo perché esteso l'ambito soggettivo dell'obbligo di notifica ma anche perché si assiste ad una maggiore esposizione agli attacchi informatici
3. Violazioni che possono presentare diversi livelli di gravità: da una grave vulnerabilità ad una errata configurazione di sistemi informatici ad errori umani (es. scambi referti, ecc.)

T4DATA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

La notifica di una violazione di dati personali (cd Data Breach)



1. La notifica ha una gestione tecnica che verifica se la violazione è stata determinata da cause tecniche o connessa ad incidenti informatici, se è ancora in essere, se sono state ripristinate tutte misure idonee ad evitare il ripetersi della violazione e se ricorre la necessità di informare gli interessati
2. A seguire il fascicolo è trasmesso al dipartimento di competenza per le proprie valutazioni
3. Il dipartimento competente verifica se sussistono violazioni della normativa vigente, se del caso avviando una istruttoria con richiesta di informazioni o nei casi più rilevanti disponendo una attività ispettiva cui potrà seguire l'avvio di un procedimento per l'adozione di provvedimenti correttivi e sanzionatori

GDPR
GENERAL DATA PROTECTION REGULATION

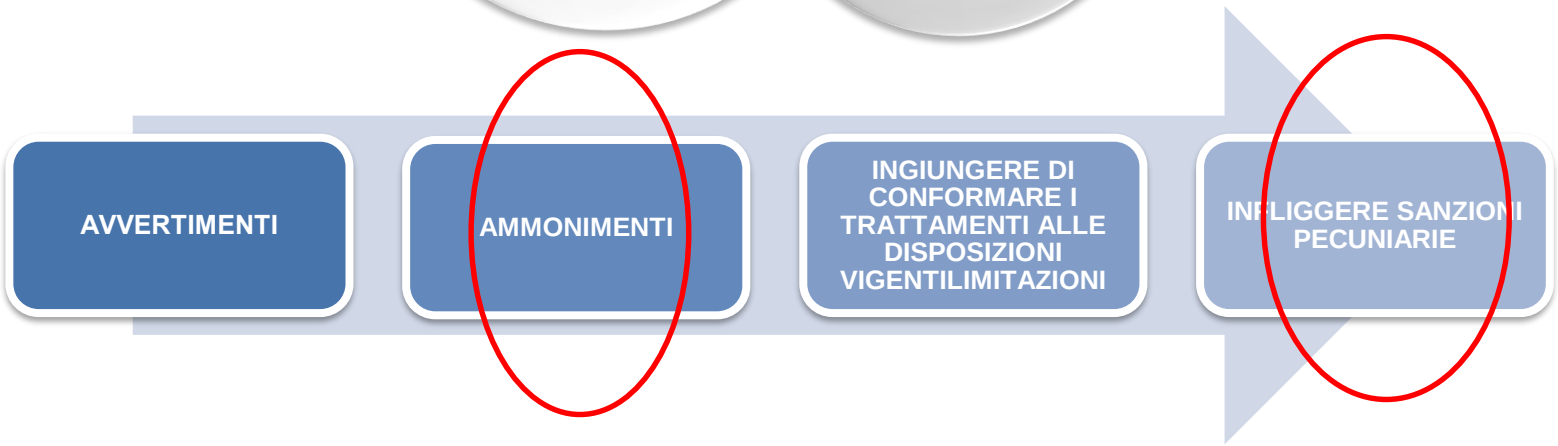
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimenti del Garante conclusivi del procedimento avviato ai sensi dell'art. 166 del Codice

Il Garante è competente ad adottare

I provvedimenti correttivi di cui all'art. 58 e le sanzioni di cui all'art. 83 del RGPD

Linee Guida WP253 3 ottobre 2017 (principio di equivalenza negli gli Stati Membri



Le autorità di controllo sono incoraggiate a ricorrere a misure correttive e sanzionatorie con un approccio ponderato ed equilibrato, al fine di reagire in maniera effettiva, dissuasiva e proporzionata alla violazione con valutazione da condurre caso per caso

Ammonimenti (Cons. 148 e Linee Guida WP 253 del 3 ottobre 2017)

Ammonimenti

1. Per **violazione minore** o se la sanzione pecuniaria dovesse costituire un onere sproporzionato, può essere rivolto un ammonimento anziché una sanzione pecuniaria
2. Il **considerando 148** introduce la **nozione** di "**violazioni minori**"
   - possono consistere nella violazione di una o più disposizioni del regolamento elencate all'articolo 83, paragrafo 4 o 5.
   - nella individuazione delle violazioni minori, l'Autorità deve considerare tutti gli elementi dell'art. 83, par. 2 del RGPD:
     - ✓ alla **natura**, alla **gravità** e alla **durata della violazione**
     - ✓ al **carattere doloso o colposo** della **violazione**
     - ✓ alle **misure adottate** per **attenuare** il **danno** subito
     - ✓ al **grado di responsabilità** o eventuali **precedenti violazioni** pertinenti
     - ✓ alla **maniera** in cui l'autorità di controllo **ha preso conoscenza della violazione**
     - ✓ al **rispetto dei provvedimenti** disposti nei confronti del titolare del trattamento o del responsabile del trattamento,
     - ✓ all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti
   - La valutazione dei criteri può spingere l'autorità di controllo a ritenere che nelle circostanze concrete la violazione, ad esempio, non crei un rischio significativo per i diritti degli interessati in questione e non incida sull'essenza dell'obbligo posto in capo al titolare
   - In tali casi, la sanzione può essere sostituita (ma non sempre) da un ammonimento

Sanzioni pecuniarie

Sanzioni

effettive **proporzionate** **dissuasive**

Linee Guida WP253 3 ottobre 2017 (principio di equivalenza negli gli Stati Membri

E al momento della loro applicazione vanno valutati tutti gli elementi dell'art. 83. par. 2 RGPD

La violazione delle disposizioni seguenti è soggetta a sanzioni amministrative previste dall'art. 83, par. 4

- **8 (Consenso dei minori)**
- **11 (Trattamento che non richiede l'identificazione)**
- **25 (*Protezione dei dati fin dalla progettazione)***
- **26 (*Contitolari del trattamento)***
- **27 (*Rappresentanti di titolari del trattamento non stabiliti nell'Unione)***
- **28 (*Responsabile del trattamento)***
- **29 (*Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento)***
- **30 (*Registri delle attività di trattamento)***
- **31 (*Cooperazione con l'autorità di controllo)***
- **32 (*Sicurezza del trattamento)***
- **33 (*Notifica di una violazione dei dati personali all'autorità di controllo);***

Sanzioni pecuniarie

Sanzioni

La violazione delle disposizioni seguenti è soggetta a sanzioni amministrative previste dall'art. 83, par. 5

i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9

i diritti degli interessati a norma degli articoli da 12 a 22

i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49

qualsiasi obbligo ai sensi delle legislazioni degli Stati adottate a norma del capo IX

l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

Alcuni suggerimenti da seguire durante le istruttorie dell'Autorità

1. Rispettare le scadenze indicate nelle comunicazioni dell'Autorità (richieste di elementi/informazioni, atto di avvio del procedimento ex art. 166 del Codice
2. Altrimenti, meglio chiedere formalmente una proroga, motivandola
3. Prestare particolare attenzione alle istruttorie per violazione dei diritti degli interessati
4. Produrre la documentazione richiesta, solo quella pertinente, evidenziando le parti rilevanti per l'istruttoria
5. Non è considerato comportamento collaborativo produrre nel procedimento documentazione non pertinente ed eccedente rispetto all'oggetto del procedimento
6. Produrre documenti volti a dimostrare la cessazione della condotta contestata ovvero il ripetersi della stessa in termini di nuovi processi, procedure tecniche, organizzative, formazione, ecc in ossequio al principio di *accountability*
7. Chiedere di essere auditi per rappresentare ulteriori elementi a difesa