PRIVACY E STUDI MEDICI

La diligenza del medico per il rispetto della privacy nella professione e verso il paziente

Relazione dell'Avv. Gennaro Messuti, Avvocato del Foro di Milano

Milano, sabato 12 maggio 2018

Sommario

Via Lamarmora, 40 - 20122 Milano
tel. 025469351 – fax 025463525
e-mail: gmessuti@inwind.it

Premessa

Il diritto alla riservatezza consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano tuttavia giustificate da interessi pubblici preminenti. Tale diritto non solo trova implicito fondamento nel sistema, ma trova una serie di espliciti riferimenti nelle norme costituzionali e ordinarie e in molteplici deliberazioni di carattere internazionale (Cass. civ., 27/05/1975, n. 2129).

Già nel 1975 la Cassazione prendeva decisa e diretta posizione nei confronti del diritto alla riservatezza.

Dopo importanti precedenti[1], il diritto alla riservatezza ha subito una manifestazione di esterofilia divenendo, in occasione dell'entrata in vigore della normativa sui dati personali, il "diritto alla privacy" al punto che quella normativa (Decreto legislativo 30 giugno 2003, n. 196) è identificata come "codice della privacy".

A tale normativa nazionale si sovrappone[2] il Regolamento Europeo del 27 aprile 2016, n. 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, pubblicato nella G.U.U.E. 4 maggio 2016, n. L 119 entrato in vigore il ventesimo giorno successivo alla pubblicazione, ma applicabile a decorrere da 25 maggio 2018 (onde permettere ai vari Stati dell'Unione Europea di adeguarsi).

La necessità di emanare un Regolamento Europeo in materia di privacy nasce dalla continua evoluzione degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente alla diffusione del progresso tecnologico.

È diventato, quindi, necessario instaurare un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione che, affiancato da efficaci misure di attuazione, consentirà lo sviluppo dell'economia digitale nel mercato interno, garantirà alle persone fisiche il controllo dei loro dati personali e rafforzerà la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche.

---

[1] La Gazzetta Ufficiale ha pubblicato l'8 gennaio 1997 con il n. 675, il testo della legge sulla "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".

[2] La Legge 25 ottobre 2017, n. 163, recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea – Legge di delegazione europea 2016-2017", provvede a dare attuazione a ben 28 direttive europee. In particolare, la delega conferita al Governo riguarda, per quanto qui di interesse, adeguamento della normativa nazionale alle disposizioni relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (Regolamento europeo n. 2016/679) e alla libera circolazione dei medesimi. L'art. 13 della Legge 163, infatti, ha investito il legislatore delegato del compito di "abrogare espressamente le disposizioni del codice (…) incompatibili con le disposizioni recate dal regolamento (UE) 2016/679" (e non il codice tutto).

Tra i principi di maggiore rilevanza meritano un particolare approfondimento il principio di trasparenza, il diritto all'oblio, il principio di accountability, il principio della privacy by design.

Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano facilmente accessibili e di facile comprensione e che sia utilizzato un linguaggio semplice e chiaro. Il responsabile del trattamento deve fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in forma intelligibile, con linguaggio semplice e chiaro e adeguato all'interessato, in particolare se le informazioni sono destinate ai minori.

Riguardo il riconoscimento del diritto all'oblio ogni persona deve avere il diritto di rettificare i dati personali che la riguardano e il "diritto alla cancellazione e all'oblio", se la conservazione di tali dati non è conforme al Regolamento.

In virtù del principio di accountability il Regolamento dispone che il responsabile del trattamento adotta politiche e attua misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme allo stesso Regolamento. Il termine anglosassone non è facilmente traducibile e difatti nella traduzione del Regolamento europeo si parla impropriamente di "responsabilità". Al massimo la traduzione più corretta, anche se poco pratica, potrebbe essere quella di "rendicontazione".

Principi generali

Il Medico tratta non solo dati personali (es. nome, cognome, indirizzo, numero di telefono, codice fiscale), ma anche dati sensibili (quelli relativi alla salute), la cui raccolta e trattamento necessita del consenso degli interessati.

Per coloro (in generale, imprese, enti privati e pubblici, professionisti) che in effetti hanno sempre prestato attenzione alle esigenze di riservatezza e protezione dei dati, sforzandosi di attuare ed attuando le misure richieste dalla normativa (non solo del Testo Unico, D.Lgs. 196/03, ma anche dei numerosi e tutt'altro che irrilevanti Provvedimenti del Garante), probabilmente sarà sufficiente programmare e implementare alcune modifiche.

Occorre in ogni caso richiamare le definizioni in materia per meglio chiarire i termini usati in modo specifico nel regolamento:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «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;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso,

mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «dati genetici»: i dati personali 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;

14) «dati biometrici»: i dati personali 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, quali l'immagine facciale o i dati dattiloscopici;

*15) «**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 informazioni relative al suo stato di salute;*

La raccolta dei dati da parte del Medico deve avvenire *nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato* secondo un principio di necessità *riducendo al minimo l'utilizzazione di dati personali e di dati identificativi*, nonché "in modo lecito, corretto e trasparente, … esatti, … aggiornati, … trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)" (art.5 reg.).

Delle misure di sicurezza e responsabilità

L'art. 32 del reg. prevede l'adozione di *misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

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

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Stante la presenza di varie figure preposte al trattamento, è previsto che *Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*

Quanto agli obblighi e alle responsabilità, *il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario* (art.24). Ad esempio, prendendo spunto dal passato, i dati personali oggetto di trattamento sono custodendi e controllandi, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Infatti, l'art.25 prevede che "*il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*".

In concreto, il Medico oggigiorno ricorre prevalentemente a strumenti elettronici per il trattamento dei dati personali, per i quali occorrono specifiche cautele che possono indicarsi (non esaustivamente):

credenziali di autenticazione *che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti, consistenti in un* ***codice per l'identificazione dell'incaricato associato a una parola chiave riservata*** *conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave;*

assegnare ad ***ogni incaricato*** *individualmente una o più credenziali per l'autenticazione;*

la ***parola chiave****, quando è prevista dal sistema di autenticazione, dovrebbe essere composta da almeno otto caratteri, non contenere riferimenti agevolmente riconducibili all'incaricato e modificata e almeno ogni tre/sei mesi;*

impartire istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;

i dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di ***idonei strumenti elettronici*** *da aggiornare con cadenza almeno semestrale.*

Se invece i trattamenti sono effettuati <u>*senza l'ausilio di strumenti elettronici*</u>, le misure di sicurezza possono essere le seguenti:

*Agli **incaricati** sono impartite **istruzioni scritte** finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

*Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono **controllati e custoditi** dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.*

***L'accesso agli archivi** contenenti dati sensibili o giudiziari è **controllato**. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.*

Del registro

Il Regolamento contiene un ritorno al passato, un ritorno dell'uguale: *ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un **registro delle attività di trattamento** svolte sotto la propria responsabilità* (art.30). Come è noto il Codice prevedeva all'art.34 c.1 lett.g) la *tenuta di un aggiornato documento programmatico sulla sicurezza*, soppresso dal D.L. 9 febbraio 2012, n. 5, convertito L. 4 aprile 2012, n. 35.

E' così costituito in capo al titolare un obbligo di documentazione della conformità della propria organizzazione alle prescrizioni della legge. Obbligo che grava anche sul responsabile, per i trattamenti che questi svolga per conto di un titolare.

Il registro non è obbligatorio per le *imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano … non sia occasionale o includa il trattamento di dati sensibili (salute).*

Poiché indiscutibilmente il medico (singolo o associato) tratta dati sensibili, il registro è un obbligo.

In ogni caso, per valutare la necessità della tenuta del registro si verifichino le seguenti domande:

1. L'organizzazione ha un numero di dipendenti pari o superiore a 250?
2. Sono effettuati trattamenti che possono presentare un rischio per i diritti e le libertà degli interessati?
3. In caso di risposta negativa al quesito n. 1) ma affermativa al n. 2), il trattamento è occasionale?
4. In caso di risposta negativa al quesito n. 1) ma affermativa al n. 2), il trattamento include "categorie particolari di dati di cui all'articolo 9, paragrafo 1 (che sono gli odierni dati sensibili, con l'aggiunta dei dati genetici e bio-

metrici), o i dati personali relativi a condanne penali e a reati di cui all'articolo 10"?

5. Contiene il registro il nome e i dati di contatto del titolare del trattamento?
6. Sono indicati il nome e i dati di contratto, ove sussistenti:
   ...del contitolare del trattamento?
   ...del rappresentante del titolare del trattamento?
   ...del responsabile della protezione dei dati?
7. Sono esplicitate le finalità dei trattamenti effettuati?
8. Per ciascun trattamento sono individuate le categorie di interessati (ad es., dipendenti, clienti/utenti, fornitori, ecc.)?
9. Per ciascun trattamento sono individuate le categorie di dati, sono cioè rintracciati:
   dati che rivelano l'origine razziale o etnica (art. 9)?
   dati che rivelano le opinioni politiche (art. 9)?
   dati che rivelano le convinzioni religiose o filosofiche (art. 9)?
   dati che rivelano l'appartenenza sindacale (art. 9)?
   dati genetici (artt. 4, par. 1, n. 13 e 9)?
   dati biometrici (artt. 4, par . 1, n. 14 e 9)?
   dati relativi alla salute (artt. 4, par. 1, n. 15 e 9)?
   dati relativi alla vita/orientamento sessuale (art. 9)?
   dati relativi a condanne penali e reati (art. 10)?
10. Per ciascun trattamento sono indicate le categorie di destinatari, cui i dati sono o saranno comunicati?

Il Gruppo di lavoro ex Articolo 29[3] ha pubblicato un parere sul registro dei trattamenti. Nel parere precisa che è sufficiente che occorra una sola delle condizioni previste dall'articolo 30 per far scattare l'obbligo di tenuta del registro. Per cui basta trattare dati personali in modo stabile per essere tenuti alla registrazione dei trattamenti. I liberi professionisti trattano -generalmente- dati personali altrui in maniera non occasionale.

Tale interpretazione appare in contrasto con quella dell'Autorità di controllo italiana che ha precisato sul suo sito che tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. In tal senso sarebbe sufficiente avere meno di 250 dipendenti e non effettuare trattamenti a rischio, laddove

[3] Il Gruppo è stato istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta.

l'interpretazione del WP29 (che è successiva, e il Garante italiano fa parte del WP29) è molto più restrittiva.

Tuttavia il contenuto dei due registri varia in relazione al soggetto tenuto all'obbligo:

- TITOLARE DEL TRATTAMENTO:
  a) *il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;*
  b) *le finalità del trattamento;*
  c) *una descrizione delle categorie di interessati e delle categorie di dati personali;*
  d) *le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*
  e) *ove applicabile, i trasferimenti di dati personali verso un paese terzo …;*
  f) *ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;*
  g) *ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1*[4].
- RESPONSABILE DEL TRATTAMENTO:
  a) *il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;*
  b) *le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;*
  c) *ove applicabile, i trasferimenti di dati personali verso un paese terzo …;*
  d) *ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.*

Ovviamente, i registri di cui sopra sono tenuti **in forma scritta**, anche in formato **elettronico.**

[4] **Articolo 32 Sicurezza del trattamento**

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

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

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Responsabile della protezione dei dati (Data Protection Officer DPO)

Oltre alle misure "tecniche", il Regolamento (art.37) ai fini della tutela e sicurezza dei dati, ha introdotto una figura nuova, quella del c.d. **Responsabile della protezione dei dati (Data Protection Officer DPO)** (che è diverso dal tecnico che segue il software), con compiti (art.39) consultivi, di assistenza e di vigilanza del rispetto della disciplina del regolamento UE sulla privacy, che tuttavia – come vedremo – non è chiaro se necessaria per il medico, o quantomeno per certe categorie.

Innanzitutto il DPO, *dipendente o con contratto di servizi,* è designato, *in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39,* dal *titolare e/o dal responsabile del trattamento ogniqualvolta* - per quanto qui di interesse - *le attività principali di questi consistono nel trattamento, su* ***larga scala****, di categorie particolari di dati personali tra cui dati relativi alla salute.*

Si rammenta che la funzione di RPD può essere svolta da un fornitore esterno di servizi e non deve necessariamente essere un dipendente effettivo dello studio medico-odontoiatrico, purché la funzione sia esercitata sulla base di un contratto stipulato tra il titolare dello studio ed una persona fisica oppure giuridica (Art. 36 GDPR), quindi una società.

Ai fini dell'individuazione dell'obbligo in capo al medico di nominare il DPO, occorre chiarire il concetto di "larga scala". Infatti, mentre per i soggetti pubblici è sempre obbligatoria la designazione del DPO (con l'eccezione delle autorità giurisdizionali), per i soggetti privati (i.e. medico) l'obbligo vale invece solo in casi particolari, quando cioè le attività principali svolte consistono nel trattamento su larga scala di dati sensibili.

Il problema è l'assoluta vaghezza e indeterminatezza del regolamento Ue, che non definisce il concetto di larga scala e gli altri requisiti valutativi della norma specifica (art.37).

È quindi stata necessaria una riunione plenaria del "Gruppo di lavoro *ex* art. 29", ossia dell'organismo consultivo che riunisce (tra l'altro) i Garanti europei, per partorire il pacchetto di linee guida sul cd. Regolamento Generale sulla Protezione dei Dati ("RGPD"), del 13 dicembre 2016 successivamente integrata il 5/4/17.

Eloquente è il disorientamento che deriva dalla lettura del § 2.1.3. sul tentativo di specificare il concetto di "larga scala":

In base all'articolo 37, paragrafo 1, lettere b) e c) del RGPD, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando

91 fornisce indicazioni in proposito.[5] *In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il WP29 intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina di un RPD. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:*

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

- la durata, ovvero la persistenza, dell'attività di trattamento;

- la portata geografica dell'attività di trattamento.

- *Alcuni esempi di trattamento su larga scala sono i seguenti:*

  - trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;

  - trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);

  - trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;

  - trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;

  - trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;

  - trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

- *Alcuni esempi di trattamento **non** su larga scala sono i seguenti:*

  - trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;

---

[5] Il considerando in questione vi ricomprende, in particolare, "*trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*". D'altro canto, lo stesso considerando prevede in modo specifico che "*Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato*". Si deve tener conto del fatto che il considerando offre alcune esemplificazioni ai **due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che fra tali estremi si colloca un'ampia zona grigia.** Inoltre, va sottolineato che il considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un RPD negli stessi identici termini.

- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Da ciò può quindi affermarsi innanzitutto che non può parlarsi di larga scala nel caso di attività svolta da un professionista individuale.

Tuttavia rimane aperto il problema se una grande farmacia, un'associazione tra professionisti o uno studio medico particolarmente strutturati possano rientrare o no, a seconda dei casi, nel concetto del trattamento su larga scala.

Si potrebbe rinvenire un aiuto nel successivo § 2.2. dove, incidentalmente, la "piccola azienda a conduzione familiare" viene esclusa dall'obbligo. E per le altre imprese? Si richiama la nozione di PMI precisata a livello europeo in base a parametri oggettivi indicati nella raccomandazione n. 2003/361/CE: *si definisce PMI, e nel dettaglio microimpresa, piccola impresa e media impresa, l'impresa che a seguito della verifica dello status di associata, collegata o autonoma, rientra nei parametri in tabella.*

	micro impresa	**piccola impresa**	**media impresa**
a) dipendenti	meno di 10	meno di 50	meno di 250
b) fatturato	non superiore a € 2 milioni	non superiore a € 10 milioni	non superiore a € 50 milioni
	oppure	*oppure*	*oppure*
c) totale di bilancio	non superiore a € 2 milioni	non superiore a € 10 milioni	non superiore a € 43 milioni

Data questa ripartizione, certamente si può dire che difficilmente medicine in rete e medicine di gruppo possano raggiungere i valori reddituali di cui alla tabella.

Anche nella medicina di rete o di gruppo i dati trattati non può dirsi che siano su larga scala: infatti, il criterio preponderante – oltre a quello economico – è quello territoriale: difficilmente una simile associazione potrà avere confini territoriali così vasti e un numero così elevato di pazienti da richiedere la nomina di un DPO. Soprattutto in considerazione del fatto che occorre fare riferimento al numero effettivo di pazienti (ossia a quei soggetti che entrano in contatto personale col loro medico) e non al numero dei pazienti potenziali (ossia agli iscritti).

Ad ogni modo, il Working Party raccomanda di tenere conto, in particolare, dei seguenti fattori:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;

- la portata geografica dell'attività di trattamento.

Occorre rilevare che le linee guida richiamano criteri basati più sul volume del trattamento (come numero degli interessati, volume dei dati personali trattati e/o loro ampiezza tipologica, durata del trattamento, contesto geografico di quest'ultimo) che sulle dimensioni della struttura. Tra gli esempi forniti di trattamento su larga scala figurano quelli di un ospedale (privato), di un'assicurazione o una banca, di un servizio di trasporto pubblico su abbonamento, di fornitori di telefonia o di servizi Internet.

Il 26 marzo 2018, il Garante italiano ha rilasciato un documento molto interessante, che contribuisce a rendere pian piano più chiaro il quadro del GDPR in vista della data fatidica del 25 maggio: una serie di domande a risposte più frequenti (FAQ) attorno alla figura del Responsabile per la Protezione dei Dati (DPO) in ambito privato.

Il terzo punto riguarda l'aspetto spinoso dell'obbligatorietà nella designazione: **i soggetti che** come "core business", ossia come attività principale, **hanno trattamenti che richiedono il "monitoraggio regolare e sistematico"[6] degli interessati su *larga scala***, o trattamenti su ***larga scala*** di categorie particolari di dati personali o di dati relativi a condanne penali e reati, devono nominare un DPO[7]. Si fa l'esempio,

[6] Per quanto riguarda il concetto di **regolare e sistematico monitoraggio dei dati** ci si riferisce a tutti i sistemi di profilazione e tracciamento automatico dell'utente che, per esempio, possono essere effettuati tramite: i network di telecomunicazioni; l'email retargeting; la profilazione del cliente per scopi assicurativi, bancari, etc; la geolocalizzazione tramite mobile app; i programmi fedeltà; il marketing comportamentale (tipico di google e dei social media) e tutta quella nuova frontiera che riguarda i wearable devices per il monitoraggio dello stato di salute e delle performance fisiche nonché l'elaborazione delle informazioni derivanti dagli oggetti interconnessi (noto anche come IOT o internet of things). In ogni caso i criteri su cui basarsi per valutare la sistematicità e regolarità del trattamento sono: la periodicità e la durata con cui questo viene effettuato, se è svolto in modo metodico, organizzato, sistematico, inserito all'interno di un progetto di raccolta ed elaborazione dei dati e all'interno di una specifica strategia aziendale.

A ciò è estraneo il gruppo o la rete di medicina.

[7] **3. Chi sono i soggetti privati obbligati alla sua designazione?**

Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Si tratta di soggetti le cui principali attività (in primis, le attività c.d. di "core business") consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala** di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).

Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; **società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione**; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

con riferimento alle categorie obbligate a nominarlo, di istituti di credito, imprese assicurative, sistemi di informazione creditizia, società finanziarie, società di informazioni commerciali, società di revisione contabile, società di recupero crediti, istituti di vigilanza, partiti e movimenti politici, sindacati, caf e patronati, società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas), imprese di somministrazione di lavoro e ricerca del personale, società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, **laboratori di analisi mediche e centri di riabilitazione**, società di call center, società che forniscono servizi informatici e società che erogano servizi televisivi a pagamento.

Circa i **soggetti che**, invece, **non saranno obbligati alla nomina**,[8] nelle FAQ si fa cenno a trattamenti effettuati da liberi professionisti operanti in forma individuale, ad agenti, rappresentanti e mediatori operanti non su ***larga scala***, ad imprese individuali o familiari, a piccole e medie imprese con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.

Viene però comunque "suggerita", in un'ottica di responsabilità, la nomina anche se la norma non la prevede come obbligatoria, per garantire un più alto livello di sicurezza.

Alla luce di quanto detto, si può concludere che – in mancanza ed aspettando specifiche da parte del Garante – per i medici in rete o in gruppo non è necessaria la nomina di un Dpo non avendo costoro un **"monitoraggio regolare e sistematico" degli interessati su *larga scala*** come le società finanziarie, ecc., essendo più vicini alle piccole e medie imprese.

Quindi non solo se la condivisione è dei soli locali in cui ogni medico è responsabile del trattamento dei propri dati con strumenti individuali e i colleghi operano quali sostituti, ma anche se invece i medici condividono i dati in unico software e/o server e li scambiano in strutture di presa in carico sempre circoscritte territorialmente (il volume dei dati va considerato in relazione ai pazienti effettivi e non potenziali).

---

[8] **4. Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?**

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti **in forma individuale**; agenti, rappresentanti e mediatori operanti non su larga scala; **imprese individuali o familiari; piccole e medie imprese**, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria").

In ogni caso, resta comunque raccomandata, anche alla luce del principio di "accountability" che permea il Regolamento, la designazione di tale figura (v., in proposito, le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

Né semplifica il Garante della Privacy.

Come detto, secondo il *Considerando 91* gli studi medici, odontoiatrici e professionali con un solo titolare del trattamento dei dati personali dei pazienti non sono obbligati a nominare un RPD. Tuttavia, se lo studio medico è convenzionato con il SSN, il Garante della Privacy raccomanda fortemente di nominare un RPD: " Occorre, comunque, considerare che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un RPD. In ogni caso, qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria"[9].

Tuttavia si tratta di una mera raccomandazione, e non di un obbligo, tant'è che in proposito il Garante parla di "designazione di un RPD su base volontaria".

Della informativa al paziente e altri diritti/doveri

L'informativa

L'informativa, in base all'articolo 13, può essere fornita in <u>forma orale o scritta</u> (anche se è preferibile la forma scritta) e deve essere preventiva rispetto al trattamento dei dati in modo da consentire al titolare dei dati di poter scegliere con consapevolezza se prestare o no il suo consenso al trattamento.[10]

> ***Articolo 13*** *Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*
>
> *1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:*
>
> *a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;*
>
> *b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;*
>
> *c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;*
>
> *d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;*

[9] "Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29)", in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110#2

[10] Esempio: «i dati raccolti saranno trattati mediante modalità cartacee o supporti informatici nel rispetto della legge sulla privacy, e verranno usati per i seguenti scopi: assistenza tecnica e post vendita, invio di materiale pubblicitario, analisi statistica di custumer satisfaction, invio di comunicazioni di carattere amministrativo, adempimento di obblighi fiscali e legali».

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Come deve essere fornita l'informativa? Al momento, possiamo ricordare l'art.42 dello SCHEMA DI DECRETO LEGISLATIVO RECANTE 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 PERSO-

NALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI E CHE ABROGA LA DIRETTIVA 95/46/CE (REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI):

Art. 42 (Informazioni del medico di medicina generale o del pediatra)

1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati negli articoli 13 e 14 del Regolamento.

2. Le informazioni possono essere fornite per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.

3. Le informazioni possono riguardare, altresì, dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto

4. Le informazioni, se non è diversamente specificato dal medico o dal pediatra, riguardano anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

a) sostituisce temporaneamente il medico o il pediatra;

b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;

c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;

d) fornisce farmaci prescritti;

e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.

5. Le informazioni rese ai sensi del presente articolo evidenziano analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

a) per scopi di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;

b) nell'ambito della teleassistenza o telemedicina;

c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica;

d) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

e) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221 del 2012.

In passato, vigente il Codice, il Garante, prendendo più consapevolezza dell'attività del MMG e del PLS, aveva ritenuto opportuno, per l'indicazione degli elementi essenziali che costoro devono includere nell'informativa da fornire all'interessato, emanare un apposito Provvedimento (19 luglio 2006) titolato **Informativa semplificata per medici di base.**

In tale documento il Garante, consultate le realtà rappresentative delle predette categorie individuate sulla base degli accordi collettivi nazionali (sindacati) nonché la Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri (FNOMCeO), ha elaborato un modello di informativa, che potrà essere utilizzato facoltativamente dai medici di medicina generale e dai pediatri di libera scelta, tenendo presente e ribadendo la funzione di tali medici, ed in particolare che:

a) le informazioni relative allo stato di salute dei pazienti possono essere rese note ai relativi familiari o conoscenti solo se gli assistiti abbiano manifestato uno specifico consenso al proprio medico. Al riguardo, l'informativa e il consenso possono intervenire anche successivamente alla prestazione nei soli casi, individuati selettivamente dal medico, di impossibilità fisica o di incapacità dell'interessato;

b) il medico di medicina generale e il pediatra di libera scelta raccolgono, di regola, i dati personali presso l'interessato e possono trattare informazioni relative ai suoi ricoveri, agli esiti di esami clinici e diagnostici (effettuati sulla base della prescrizione dello stesso medico di medicina generale o del pediatra) solo quando l'interessato abbia manifestato alla struttura sanitaria o al professionista presso cui si è rivolto il suo consenso.

L'allegato modello di informativa riguarda anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, svolto da ***un professionista o da altro soggetto, individuabile in base alla prestazione richiesta****. Tale trattamento può essere in tal senso effettuato da chi sostituisca temporaneamente il medico, o fornisca una prestazione specialistica su richiesta dello stesso, oppure tratti lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata o, ancora, fornisca i farmaci prescritti o comunichi i dati personali dell'interessato al medico in conformità alla disciplina applicabile (art. 78, comma 4, del Codice).*

Gli elementi indicati nell'allegato modello di informativa possono essere forniti all'interessato nei modi di legge una tantum, attraverso idonee modalità che ne facilitino la conoscenza da parte degli assistiti, anche sulla base del rapporto personale con il singolo paziente e tenendo conto delle circostanze concrete. I contenuti dell'informativa possono essere comunicati direttamente all'assistito, ***a voce o per iscritto****,* ***oppure affiggendo il testo dell'informativa, facilmente visibile, nella sala d'attesa dello studio medico*** *ovvero con altra idonea modalità (in aggiunta o in sostituzione delle altre forme) quale, ad esempio, la riproduzione dell'informativa in carte tascabili con eventuali allegati pieghevoli (art. 78, comma 3, del Codice).*

L'informativa può essere fornita ***anche successivamente*** *alla prestazione, senza ritardo, nel caso di emergenza sanitaria o di igiene pubblica (art. 117 D.Lgs. 31 marzo 1998, n. 112), di impossibilità fisica, di incapacità di agire o di incapacità di intendere o di volere dell'interessato, di rischio grave, imminente ed irreparabile per la salute o dell'interessato o nel caso in cui la prestazione medica può essere pregiudicata in termini di tempestività o efficacia (art. 82 del Codice).*

Tali presupposti, indicati nell'art.78 del Codice della privacy, sono stati ripresi integralmente dall'art.42 dello Schema di decreto legislativo citato:

CODICE DELLA PRIVACY	SCHEMA DECRETO LEGISLATIVO
Art. 78 *(Informativa del medico di medicina generale o del pediatra)*	Art. 42 (*Informazioni del medico di medicina generale o del pediatra*)

1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati nell'*articolo 13, comma 1*.	1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati negli articoli 13 e 14 del Regolamento.
2. L'informativa può essere fornita per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.	2. Le informazioni possono essere fornite per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.
3. L'informativa può riguardare, altresì, dati personali eventualmente raccolti presso terzi, ed è fornita preferibilmente per iscritto, anche attraverso carte tascabili con eventuali allegati pieghevoli, includendo almeno gli elementi indicati dal Garante ai sensi dell'*articolo 13, comma 3*, eventualmente integrati anche oralmente in relazione a particolari caratteristiche del trattamento.	3. Le informazioni possono riguardare, altresì, dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto.
4. L'informativa, se non è diversamente specificato dal medico o dal pediatra, riguarda anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che: a) sostituisce temporaneamente il medico o il pediatra; b) fornisce una prestazione specialistica su richiesta del medico e del pediatra; c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata; d) fornisce farmaci prescritti; e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.	4. Le informazioni, se non è diversamente specificato dal medico o dal pediatra, riguardano anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che: a) sostituisce temporaneamente il medico o il pediatra; b) fornisce una prestazione specialistica su richiesta del medico e del pediatra; c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata; d) fornisce farmaci prescritti; e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.
5. L'informativa resa ai sensi del presente articolo evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati: a) per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente; b) nell'ambito della teleassistenza o telemedicina; c) per fornire altri beni o servizi all'interessato	5. Le informazioni rese ai sensi del presente articolo evidenziano analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati: a) per scopi di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente; b) nell'ambito della teleassistenza o telemedicina; c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica;

attraverso una rete di comunicazione elettronica.	d) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221; e) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221 del 2012.

Pertanto, sebbene l'art.78 cdp è stato abrogato, l'art.42 dello schema dlgs ne ha ripetuto il contenuto che aveva determinato il Garante ad adottare il provvedimento de quo.

Riportiamo il modello di informativa ancora attuale quindi:

INFORMAZIONE

Gentili signori,

desidero informarvi che i vostri dati sono utilizzati solo per svolgere attività necessarie per prevenzione, diagnosi, cura, riabilitazione o per altre prestazioni da voi richieste, farmaceutiche e specialistiche.

Si tratta dei dati forniti da voi stessi o che sono acquisiti altrove, ma con il vostro consenso, ad esempio in caso di ricovero o di risultati di esami clinici.

Anche in caso di uso di computer, adotto misure di protezione per garantire la conservazione e l'uso corretto dei dati anche da parte dei miei collaboratori, nel rispetto del segreto professionale. Sono tenuti a queste cautele anche i professionisti (il sostituto, il farmacista, lo specialista) e le strutture che possono conoscerli.

I dati non sono comunicati a terzi, tranne quando sia necessario o previsto dalla legge.

Si possono fornire informazioni sullo stato di salute a familiari e conoscenti solo su vostra indicazione.

In qualunque momento potrete conoscere i dati che vi riguardano, sapere come sono stati acquisiti, verificare se sono esatti, completi, aggiornati e ben custoditi, e far valere i vostri diritti al riguardo.

Per attività più delicate da svolgere nel vostro interesse, sarà mia cura informarvi in modo più preciso.

Il consenso

Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. ... Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. ... (Considerando 32).

Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di esprimere un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza al-

meno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio (Considerando 42).

Ciò premesso, "il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; ...[11] (Articolo 6 Liceità del trattamento)

Naturalmente, il **consenso** deve essere validamente prestato (art.7 Condizioni per il consenso):

> *1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.*
>
> *2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.*
>
> *3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.*
>
> *4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.*

---

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

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

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

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

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

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

Il diritto di accesso

Ricordiamo che l'interessato ha sempre **diritto di accesso** (art.15), cioè *di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:*

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

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

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

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

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

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

L'art.15 prevede inoltre la possibilità di *addebitare un contributo spese ragionevole basato sui costi amministrativi* e la possibilità di *fornire le informazioni in un formato elettronico di uso comune* (ma sempre nel rispetto della riservatezza, e quindi con le cautele cui è obbligato il medico) *se la richiesta è presentata mediante mezzi elettronici, salvo indicazione diversa dell'interessato.*

Sebbene non sia disciplinato, l'esercizio di tali diritti è esercitato dal paziente *senza formalità* (cfr.art.8 del Codice), *anche mediante lettera raccomandata, telefax o posta elettronica, e finanche oralmente (in tal caso la richiesta è annotata sinteticamente a cura dell'incaricato o del responsabile), personalmente o per delega o procura scritte a persone fisiche, enti, associazioni od organismi, e con l'assistenza di una persona di fiducia* (cfr.art.9 del Codice): ovviamente i richiedenti, chiunque essi siano, debbono essere riconoscibili e identificabili, altrimenti il medico può, anzi deve, rifiutarsi. *Il titolare del trattamento dovrebbe adottare tutte le misure ragionevoli per verificare l'identità di un interessato che chieda l'accesso, in particolare nel contesto di servizi online e di identificativi online. Il titolare del trattamento non dovrebbe conservare dati personali al solo scopo di poter rispondere a potenziali richieste* (considerando 64).

Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste (Considerando 59).

Diritto alla cancellazione

Il Regolamento (art.17) ha ampliato il **diritto alla cancellazione** dei dati personali (c.d. diritto all'oblio), sia perché non più necessari rispetto alle finalità di raccolta,

ovvero per revoca del consenso, ovvero perché trattati illecitamente. Tuttavia i doveri legati al "diritto all'oblio" (in particolare, internet) sono difficilmente rinvenibili in capo al medico (una sorta di *damnatio memoriae*, che nell'antica Roma comportava, quale sanzione per gravi infrazioni, la eliminazione di ogni traccia della esistenza in vita della persona condannata).

Articolo 17 *Diritto alla cancellazione («diritto all'oblio»)*

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso ...;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. ...

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) ...;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Delle persone decedute

Il § 27 dei Considerando prevede che "Il presente regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute".

Orbene, l'art.13 (*Delega al Governo 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*) della LEGGE 25 ottobre 2017, n. 163 (pubblicata nella Gazz. Uff. 6 novembre 2017, n. 259) prevede che "*Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, ... uno o più decreti legislativi al fine di adeguare il quadro normativo 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. ... Nell'esercizio della delega il Governo è tenuto a seguire ... anche i seguenti princìpi e criteri direttivi specifici:*

a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;

e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

Se il Governo si adeguerà a tali previsioni (senza incorrere nel c.d. vizio per eccesso di delega), si dovrà continuare a fare riferimento al Codice della privacy. In particolare l'art.9 stabilisce che *I diritti di cui all'articolo 7 [diritto di accesso ai dati personali e ad altri diritti] riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.*

Sul punto si è più volte espressa la giurisprudenza, chiarendo che "in tema di trattamento dei dati personali, tra i dati concernenti persone decedute, ai quali hanno diritto di accesso gli eredi, a norma dell'art. 9, comma 3, D.Lgs. n. 196 del 2003, non rientrano quelli identificativi di terze persone, quali i beneficiari della polizza sulla vita stipulata dal de cuius, ma soltanto quelli riconducibili alla sfera personale di quest'ultimo" (Cass. civ. Sez. I, 08/09/2015, n. 17790).

"*La disciplina dell'articolo 9 del codice D.Lgs. n. 196 del 2003 regola (...) compiutamente ed esaustivamente la questione del trattamento dei dati personali delle persone decedute, in*

*quanto indica **chi può esercitare** l'insieme dei diritti previsti dall'art. 7 dello stesso codice, il quale, nel disciplinare il trattamento dei dati medesimi, considera non solo le posizioni soggettive di chi può esercitare il diritto di accesso, ma anche quello di **chi può opporsi** ad esso. Si può, dunque, concludere su questo punto che sopravvive una forma di tutela dei dati sensibili - come altre forme di tutela - anche dopo la morte, ma nelle forme specifiche e diverse previste dall'art. 9, che individua puntualmente gli interessi che possono bilanciare gli interessi di terzi ad accedere ai dati personali: la tutela del defunto e ragioni familiari meritevoli di protezione" (Consiglio di Stato, III, 12 giugno 2012, n. 3459).*

Nel caso frequente di più eredi, occorre innanzitutto ribadire che il medico deve rilasciare la documentazione a chi dimostra la sua legittimazione, allegando ad esempio una dichiarazione sostitutiva di atto notorio attestante la qualità di legittimo erede e la relazione di parentela esistente con il defunto, del quale dovevano essere specificati tutti i dati anagrafici. Non è invece necessario, nel caso di più eredi, che la predetta dichiarazione sia resa da tutti: infatti, *l'accesso alla documentazione sanitaria del familiare deceduto non risulta in alcun modo pregiudizievole per gli altri eredi, non implicando alcuna "deminutio" delle prerogative ereditarie, ovvero l'esclusione di questi ultimi da informazioni utili con l'appropriazione esclusiva da parte di alcuni eredi (gli odierni ricorrenti) in danno di altri, né la disposizione di alcun diritto ereditario (Cfr. in termini, Tar Lazio, Sezione Terza, 30 gennaio 2003, n. 535). Ciò premesso, la richiesta del consenso di tutti i coeredi risulta illegittima, dal momento che i richiedenti (alcuni coeredi) sono titolari di situazioni giuridicamente tutelate e collegate ai documenti ai quali è chiesto l'accesso e che l'art. 9, comma 3, del Decreto Leg.vo 30 giugno 2003 n. 196 consente loro l'accesso* (T.A.R. Sicilia Catania Sez. IV Sent., 17/11/2007, n. 1877).

Occorre tuttavia rammentare che è allo studio uno schema di decreto legislativo[12] che letteralmente si riporta:

> *Art. 13 (Diritti riguardanti le persone decedute)*
>
> ~~1. Le disposizioni del Regolamento e del presente decreto si applicano anche ai dati personali concernenti persone decedute.~~
>
> 2. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali di cui al comma 1 possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
>
> 3. L'esercizio dei diritti di cui al comma 2 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento.

[12] SCHEMA DI DECRETO LEGISLATIVO RECANTE 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)

4. La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 2 deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.

5. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 3 e 4.

6. In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

Privacy by design e privacy by default

Sempre in ambito innovativo, il Regolamento introduce (art.25) i concetti di **Privacy by design e privacy by default:** all'atto del trattamento ovvero di determinare i mezzi del medesimo, il titolare deve approntare misure tecniche e organizzative adeguate - quali la pseudonimizzazione - in modo da attuare efficacemente i principi di protezione dei dati - quali la minimizzazione - e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento deve altresì attuare misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

I principi che reggono il sistema sono i seguenti:

- prevenire non correggere, cioè i problemi vanno valutati nella fase di progettazione;
- privacy come impostazione di default;
- privacy incorporata nel progetto;
- massima funzionalità, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = meno sicurezza);
- sicurezza durante tutto il ciclo del prodotto o servizio;
- trasparenza;
- centralità dell'utente.

L'obbligo di *privacy by design* è basato sulla valutazione del rischio che andrà fatta al momento della progettazione del sistema, quindi prima che il trattamento inizi, tenendo conto del tipo di dati trattati e dello stato della tecnologia, per cui il trattamento va adattato nel corso del tempo.

Il principio di *privacy by default* stabilisce, invece, che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

Dell'utilizzo dei dati *senza* consenso

Quanto all'utilizzazione da parte del titolare del trattamento dei dati, l'articolo 9 (Trattamento di categorie particolari di dati personali) prevede:

1. 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.

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, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per **assolvere gli obblighi ed esercitare i diritti** specifici del titolare del trattamento o dell'interessato **in materia di diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è **necessario per accertare, esercitare o difendere un diritto in sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di **interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla prote-

zione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per 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, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della **sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

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

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, **lettera h)**, se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al **segreto professionale** conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

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.

Va tuttavia osservato che "il problema di una comparazione di interessi confliggenti non si pone allorquando l'accesso si riferisca a cartelle cliniche di persone decedute, dato che il diritto alla riservatezza si estingue con la morte del titolare. Di talché, è irrilevante che gli istanti siano o meno titolari di un diritto 'di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile', né che siano o meno eredi effettivi del soggetto cui si riferiscono i dati. Ciò che il giudice deve accertare è se gli istanti abbiano maturato 'iure proprio' il diritto all'accesso ai dati contenuti nella cartella clinica, in conformità a quanto sancito dall'art. 9, comma 3, del predetto Codice, ovvero se

siano titolari di una 'situazione giuridicamente rilevante' che li legittima a pretendere l'esibizione di atti potenzialmente capaci di giovare alla salvaguardia dei propri interessi (nella fattispecie della propria aspirazione ad una porzione di patrimonio del defunto, dalla successione del quale erano stati a loro avviso ingiustamente estromessi) (T.A.R. Lombardia Brescia Sez. II, 16/12/2011, n. 1761 confermato da Cons. Stato Sez. III, 12/06/2012, n. 3459).

Sul punto, a segnalare la difficoltà di una univoca interpretazione, sono intervenute le Sezioni Unite della Cassazione Civile (sentenza 08/02/2011, n. 3034) affermando che "non è configurabile alcuna lesione del diritto alla protezione dei dati personali qualora l'utilizzazione del dato altrui avvenga a fine di giustizia e l'atto che lo contiene risulti essere stato posto in essere nell'osservanza del codice di rito. In tema di protezione dei dati personali, non costituisce violazione della relativa disciplina il loro utilizzo mediante lo svolgimento di attività processuale giacché detta disciplina non trova applicazione in via generale, ai sensi degli artt. 7, 24 e 46-47 del d.lgs. n. 193 del 2003 (cd. codice della privacy), quando i dati stessi vengano raccolti e gestiti nell'ambito di un processo; in esso, infatti, la titolarità del trattamento spetta all'autorità giudiziaria e in tal sede vanno composte le diverse esigenze, rispettivamente, di tutela della riservatezza e di corretta esecuzione del processo, per cui, se non coincidenti, è il codice di rito a regolare le modalità di svolgimento in giudizio del diritto di difesa e dunque, con le sue forme, a prevalere in quanto contenente disposizioni speciali e, benché anteriori, non suscettibili di alcuna integrazione su quelle del predetto codice della privacy".

Del regime sanzionatorio

Risarcimento del danno

Con l'entrata in vigore del GDPR, il quadro sanzionatorio privacy è ben più severo.

Sulla base dell'art. 82 del GDPR, resta fatta la salva la possibilità per l'interessato, che subisca un danno materiale o immateriale, di ottenere il risarcimento del danno, a seconda che la violazione sia stata commessa dal Titolare o dal Responsabile.

> 1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
>
> 2. Un *titolare del trattamento* coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un *responsabile del trattamento* risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso **non gli è in alcun modo imputabile**.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è **responsabile in solido** per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle **autorità giurisdizionali competenti** a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Sanzioni amministrative pecuniarie

Il GDPR, agli articoli successivi, invece, disciplina le ipotesi per cui è prevista l'applicazione di **sanzioni amministrative pecuniarie** e/o penali. Per quanto riguarda le prime esse possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale nei casi di, a titolo esemplificativo:

- ✓ violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- ✓ trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- ✓ mancata o errata notificazione e/o comunicazione di un data breach all'Autorità nazionale competente;
- ✓ violazione dell'obbligo di nomina del DPO;
- ✓ mancata applicazione di misure di sicurezza.

L'importo delle sanzioni amministrative pecuniarie può salire fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato mondiale dell'impresa nei casi di, a titolo esemplificativo:

- ✓ inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- ✓ trasferimento illecito cross-border di dati personali ad un destinatario in un Paese terzo.

All'interno del GDPR è presente anche un margine di **discrezionalità** circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa. Ciò non implica un'autonomia gestionale delle sanzioni in capo alle Autorità nazionali competenti, ma fornisce, a queste ultime, alcuni criteri su come interpretare le singole circostanze del caso (articolo 83 paragrafo 2[13]):

la natura, gravità e durata della violazione

Con riferimento al primo criterio, lo stesso regolamento riconosce l'esistenza di diversi massimali per le sanzioni amministrative pecuniarie, 10 o 20 milioni di euro. All'interno del Considerando 148, è offerta all'Autorità nazionale l'opportunità di sostituire la sanzione pecuniaria con un ammonimento, "in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica".

il carattere doloso o colposo della violazione

Con riferimento a tale criterio, in attesa delle valutazioni giurisprudenziali, il Gruppo di Lavoro art.29 ha, tuttavia, già provveduto ad esemplificare alcune condotte che potranno integrare il suddetto carattere doloso. Queste sono riconducibili alle ipotesi di:

- ✓ trattamenti illeciti autorizzati esplicitamente dal senior management, ovvero ignorando i pareri formulati dal DPO;

---

[13] Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

- ✓ modifica di dati personali, avente la finalità di fornire un'impressione "fuorviante" circa il conseguimento degli obiettivi individuati;
- ✓ vendita di dati, in mancanza di verifica e/o ignorando la scelta liberamente esercitata dagli interessati.

Anche all'interno delle presenti linee guida viene, inoltre, precisato che la carenza di risorse economiche e materiali non potrà costituire ipotesi di esenzione di responsabilità. In funzione del cosiddetto *risk based approach*, infatti, il titolare dovrà progettare, sin dal principio, il proprio trattamento, stimando l'esistenza di possibili rischi per i diritti e le libertà degli interessati. Tale valutazione iniziale determinerà l'entità della responsabilità, in capo al Titolare o al suo Responsabile, tenendo in considerazione il contesto, le finalità e la natura del trattamento.

il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi

Questo criterio potrà costituire un fattore determinante, nella scelta di applicare o meno una sanzione amministrativa e, eventualmente, fissarne l'ammontare, qualora siano state limitate o azzerate le ripercussioni negative sui diritti degli interessati che si sarebbero altrimenti verificate in mancanza di tale collaborazione.

Sanzioni penali

Nonostante il GDPR focalizzi la propria attenzione, prevalentemente, sulle violazioni di tipo amministrativo, all'interno del Considerando 149 è stabilito che gli Stati Membri "dovrebbero poter stabilire disposizioni relative a sanzioni penali" come strumento di attuazione e tutela della nuova disciplina, pur sempre in ossequio al principio del ne bis in idem .

Alcuni casi pratici

Per concludere, soffermiamoci su alcune problematiche pratiche.

Innanzitutto occorre prestare attenzione nella comunicazione, soprattutto via internet: in tali casi è facile sconfinare nella divulgazione illegittima di dati sensibili.

La Suprema Corte con sua ordinanza n. 3455 del 9 febbraio 2017 ha disposto la rimessione degli atti al Primo Presidente per l'eventuale assegnazione del ricorso alle Sezioni Unite al fine di dirimere l'insanabile contrasto sorto in merito alla definizione e alla normativa applicabile per il trattamento e comunicazione dei dati sensibili, nel rispetto della normativa inerente la protezione dei dati personali.[14]

[14] Nel caso in esame un privato cittadino conveniva in giudizio avanti al Tribunale di Napoli la Regione Campania, il Banco di Napoli nonché il Garante per la Protezione dei Dati Personali con ricorso ex art. 152 del D. Lgs. 196/2003 per illecito trattamento dei dati personali idonei a rilevare il proprio stato di salute.

Con sentenza n. 10947/2014 la Suprema Corte, sulla medesima questione in esame, aveva rilevato l'illegittimo trattamento dei dati personali da parte della Regione e della Banca, in quanto vi era stata una diffusione di dati sensibili idonei a rivelare lo stato di salute del soggetto interessato, dovuta al mancato utilizzo di tecniche di cifratura o numeri di codice non identificabile previsti dall'art. 22 comma 6 del D. Lgs. 196/2003.

In contrasto con tale decisione la Cassazione, con sua sentenza n. 10280/2015 ha escluso che la dizione "indennizzo ex Legge 210/1992", inserita nell'ordine di bonifico e nell'estratto conto, fosse idonea a rivelare lo stato di salute dell'interessato, e in quanto tale dato sensibile, poiché proprio la Legge 210/1992, come si è detto, prevede il diritto ad un indennizzo per due categorie differenti di soggetti: coloro che hanno riportato una menomazione permanente dell'integrità psicofisica e coloro che sono prossimi congiunti di soggetti deceduti a causa di un'infezione da trasfusione o vaccinazione di cui alla Legge 210/1992.

Con la citata Ordinanza, 09/02/2017, n. 3455, la prima sezione civile ha rimesso gli atti al Primo Presidente per l'eventuale assegnazione della causa alle sezioni unite civili in relazione al contrasto sorto all'interno delle sezioni ordinarie in ordine alle nozioni e alle modalità di trattamento e di comunicazione di dati sensibili, con particolare riferimento a quei dati che possano essere indicativi delle condizioni di salute del titolare.

Occorre quindi prestare molta attenzione nella trasmissione via email di ricette, certificati, ecc.: ciò può avvenire nel rispetto delle regole sinora esposte.

Nello specifico il ricorrente, quale beneficiario di un indennizzo ai sensi della Legge 210/1992 erogato dalla Regione Campania mediante accredito sul proprio conto corrente acceso presso una filiale del Banco di Napoli, rilevava che la Regione Campania nel disporre il pagamento aveva indicato quale causale la dicitura "pagamento ratei arretrati bimestrali e posticipati Legge 210/1992" e che con la medesima definizione il Banco di Napoli aveva indicato il relativo movimento nell'estratto conto cartaceo inviato all'interessato.

Si rileva che la Legge 210/1992 riconosce un diritto ad un indennizzo a quei soggetti danneggiati da complicanze di tipo irreversibile, dalle quali sia derivata una menomazione permanente dell'integrità psico-fisica a causa di vaccinazioni obbligatorie o a causa di **infezioni da HIV** a seguito di trasfusioni, nonché agli operatori sanitari che, in occasione e durante il servizio, abbiano riportato danni permanenti alla integrità psico-fisica a seguito di contatto con sangue e suoi derivati provenienti da soggetti affetti da infezione da HIV.

Inoltre tale indennizzo è riconosciuto, una tantum, ai prossimi congiunti dei soggetti deceduti a seguito delle predette patologie.

In ragione di tale circostanza, poiché tale dicitura risulta idonea a rivelare lo stato di salute del soggetto interessato, a parere del ricorrente era stato effettuato un **illegittimo trattamento dei propri dati personali** sia da parte della Regione che della Banca, di cui chiedeva la condanna al risarcimento del danno nonché alla rimozione del dato divulgato.

La violazione della privacy del malato di HIV per esigenze di prevenzione del contagio: si può parlare di prevenzione del contagio come esimente dalla responsabilità per illecito trattamento dei dati sanitari del malato di HIV? Lo si dovrebbe potere fare se, anche in tema di responsabilità da trattamento di dati personali, fossero applicabili le esimenti generali dell'esercizio del diritto e dell'adempimento del dovere, considerato come le suddette ragioni di prevenzione appaiano agevolmente riconducibili al diritto-dovere, specialmente per il medico, di tutelare la salute propria e dei terzi in potenziale pericolo di contagio. E comunque, anche le norme contenute nel regolamento[15] fanno spesso esplicito riferimento alla necessità di salvaguardare la vita o l'incolumità fisica, dell'interessato o anche di terzi, o della collettività, quale elemento idoneo a fondare un lecito trattamento dei dati personali pure in assenza di determinati requisiti che sarebbero, invece, ordinariamente richiesti, sembrando così potere costituire la base normativa per la individuazione, in collegamento con una tale necessità, di una sorta di esimente speciale.

Si ricorda la decisione del Tribunale di Bologna (sent. del 19.5.2005 n. 1279) secondo cui «Le ragioni di prevenzione e contenimento del contagio, in ipotesi, valgono quali cause di giustificazione della lesione del diritto alla riservatezza qui lamentata ex art. 2043 c.c., poiché la qualificazione dell'ingiustizia del danno implica il vaglio comparativo degli interessi in conflitto». Il Tribunale di Bologna richiama una serie di norme e una pronuncia della Corte costituzionale, dalle quali sarebbe desumibile la necessità di bilanciare la tutela della riservatezza del malato di HIV con la prevalente esigenza di tutela della salute pubblica e privata: si tratta dell'art. 7, l. n. 135/1990, che ha introdotto una serie di norme di protezione dal contagio di HIV nelle strutture sanitarie ed assistenziali, pubbliche e private; della Direttiva n. 95/46/CE, che, all'art. 8, par. 3, – ricorda il Tribunale di Bologna – contiene una «deroga al regime ordinario del trattamento dei dati personali (...) giustificata proprio dalla preminenza accordata al diritto alla salute pubblica e alla protezione sociale rispetto al diritto alla riservatezza del singolo»; dell'art. 32 Cost. che «impone di assicurare la miglior cura del paziente e la più efficace prevenzione di conseguenze pregiudizievoli per la collettività» (sent.cit.); della sentenza della C. Cost. n. 218/1994 che ha dichiarato l'incostituzionalità dell'art. 5, 3º e 5º co., l. n. 135/1990, nella parte in cui non prevede accertamenti sanitari dell'assenza di sieropositività all'infezione da HIV come condizione per l'espletamento di attività che comportano rischi per la salute di terzi.

[15] Ad es. *art. 6 Liceità del trattamento*.

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

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

Infine, il medico deve rivelare ai consanguinei la sofferenza di patologie genetiche ereditarie del suo paziente? La soluzione, a differenza del precedente che aveva di mira la collettività, è più complessa perché riguarda singoli e identificati soggetti.

Un caso non sicuramente scolastico è il seguente, ma che riassume il problema. La questione riguarda il **bilanciamento del diritto alla riservatezza del malato** (es. padre), il quale rifiuta che venga rivelata la sofferenza della patologia con il diritto alla conoscenza e alla **salute ad esempio delle figlie**, una delle quali incinta al momento della scoperta della malattia paterna.

La tesi sfavorevole alla divulgazione della malattia sostenendo che la figlia non era parte del rapporto medico-paziente e pertanto il medico curante aveva alcun obbligo fondato sul "***dovere di diligenza***" nei suoi confronti.

La tesi opposta si fonda sul fatto che proprio l'ambito della genetica rende i terzi consanguinei giuridicamente sensibili e legittimamente interessati all'acquisizione di tali informazioni genetiche critiche, perché questi, spesso, possono diventare a loro volta pazienti, con il dovere del medico di avvisare la famiglia del paziente per il rischio di probabili malattie genetiche.

Il codice deontologico medico

In conclusione, va ricordato l'obbligo per il Medico di osservare e rispettare il Codice deontologico, la cui osservanza è richiamata anche dal Regolamento.

Come si è avuto modo di vedere ampiamente la *ratio* posta a fondamento della normativa sulla privacy è quella di contemperare le esigenze di tutela della salute (quale diritto fondamentale dell'individuo) con quelle al rispetto della dignità dell'uomo e della riservatezza.

Tali esigenze sono state fatte proprie anche dal Codice deontologico dei medici chirurgi ed odontoiatri che agli artt.10, 11 e 12 prescrivono misure da rispettarsi dagli esercenti le professioni sanitarie, rammentando la vigenza a Milano del Codice deontologico del 2006 che, come risulta dal raffronto nella tabella sottostante, risulta essere più esaustivo e completo di quello del 2014.

CODICE 2006	CODICE 2014
Art. 10 - Segreto professionale - Il medico deve mantenere il segreto su tutto ciò che gli è confidato o di cui venga a conoscenza nell'esercizio della professione. La morte del paziente non esime il medico dall'obbligo del segreto. Il medico deve informare i suoi collaboratori dell'obbligo del segreto professionale. L'inosservanza del segreto medico costituisce mancanza grave quando possa derivarne profitto proprio o altrui ovvero nocumento della persona assistita o di altri. La rivelazione è ammessa ove motivata da una giusta causa, rappresentata dall'adempimento di un obbligo previsto dalla legge (denuncia e referto all'Autorità Giudiziaria, denunce sanitarie, notifiche di malattie infettive, certificazioni obbligatorie) ovvero da quanto previsto dai successivi artt. 11 e 12. Il medico non deve rendere al Giudice testimonianza su fatti e circostanze inerenti il segreto professionale. La cancellazione dall'albo non esime moralmente il medico dagli obblighi del presente articolo.	**Art. 10 - Segreto professionale -** Il medico deve mantenere il segreto su tutto ciò di cui è a conoscenza in ragione della propria attività professionale. La morte della persona assistita non esime il medico dall'obbligo del segreto professionale. Il medico informa i collaboratori e discenti dell'obbligo del segreto professionale sollecitandone il rispetto. La violazione del segreto professionale assume maggiore gravità quando ne possa derivare profitto proprio o altrui, ovvero nocumento per la persona assistita o per altri. La rivelazione è ammessa esclusivamente se motivata da una giusta causa prevista dall'ordinamento o dall'adempimento di un obbligo di legge. Il medico non deve rendere all'Autorità competente in materia di giustizia e di sicurezza testimonianze su fatti e circostanze inerenti al segreto professionale. La sospensione o l'interdizione dall'esercizio professionale e la cancellazione dagli Albi non dispensano dall'osservanza del segreto professionale.
Art. 11 - Riservatezza dei dati personali - Il medico è tenuto al rispetto della riservatezza nel trattamento dei dati personali del paziente e particolarmente dei dati sensibili inerenti la salute e la vita sessuale. Il medico acquisisce la titolarità del trattamento dei dati sensibili nei casi previsti dalla legge, previo consenso del paziente o di chi ne esercita la tutela. Nelle pubblicazioni scientifiche di dati clinici o di osservazioni relative a singole persone, il medico deve assicurare la non identificabilità delle stesse. Il consenso specifico del paziente vale per ogni ulteriore trattamento dei dati medesimi, ma solo nei limiti, nelle forme e con le deroghe stabilite dalla legge. Il medico non può collaborare alla costituzione di banche di dati sanitari, ove non esistano garanzie di tutela della riservatezza, della sicurezza e della vita privata della persona.	**Art. 11 - Riservatezza dei dati personali -** Il medico acquisisce la titolarità del trattamento dei dati personali previo consenso informato dell'assistito o del suo rappresentante legale ed è tenuto al rispetto della riservatezza, in particolare dei dati inerenti alla salute e alla vita sessuale. Il medico assicura la non identificabilità dei soggetti coinvolti nelle pubblicazioni o divulgazioni scientifiche di dati e studi clinici. Il medico non collabora alla costituzione, alla gestione o all'utilizzo di banche di dati relativi a persone assistite in assenza di garanzie sulla preliminare acquisizione del loro consenso informato e sulla tutela della riservatezza e della sicurezza dei dati stessi.
Art. 12 - Trattamento dei dati sensibili - Al medico, è consentito il trattamento dei dati personali idonei a rivelare lo stato di salute del paziente previa richiesta o autorizzazione da parte di quest'ultimo, subordinatamente ad una preventiva informazione sulle conseguenze esuli' opportunità della rivelazione stessa. Al medico peraltro è consentito il trattamento dei dati personali del paziente in assenza del consenso dell'interessato solo ed esclusivamente quando sussistano le specifiche ipotesi previste dalla legge ovvero quando vi sia la necessità di salvaguardare la vita o la salute del paziente o di terzi nell'ipotesi in cui il paziente medesimo non sia in grado di prestare il proprio consenso per impossibilità fisica, per incapacità di agire e/o di intendere e di volere; in quest'ultima situazione peraltro, sarà necessaria l'autorizzazione dell'eventuale legale rappresentante laddove precedentemente nominato. Tale facoltà sussiste nei modi e con le garanzie dell'art. 11 anche in caso di diniego dell'interessato ove vi sia l'urgenza di salvaguardare la vita o la salute di terzi.	**Art. 12 - Trattamento dei dati sensibili -** Il medico può trattare i dati sensibili idonei a rivelare lo stato di salute della persona solo con il consenso informato della stessa o del suo rappresentante legale e nelle specifiche condizioni previste dall'ordinamento.

Riepilogo dei principali adempimenti del professionista

In conclusione, ecco un breve riepilogo dei principali adempimenti del professionista in vista dell'entrata in vigore del GDPR:

A. Predisporre la modulistica per procedere, durante il primo incontro con il Paziente, alla raccolta dei dati fornendo al medesimo una informativa completa, con un linguaggio semplice e chiaro.
B. Organizzare le proprie attività in modo da raccogliere e trattare solo ed esclusivamente i dati che sono necessari o utili in vista del miglior espletamento del mandato professionale ricevuto: si raccolgono e si trattano esclusivamente i dati personali che non siano "eccedenti" rispetto alle finalità del trattamento, ovvero che siano "limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5[16], c.d. "minimizzazione dei dati")
C. Organizzare la conservazione dei documenti relativi alle varie pratiche in modo da averne sempre, al momento giusto, la disponibilità ed in modo che i dati siano accessibili al solo personale autorizzato.
D. Nominare e adeguatamente istruire i collaboratori e formalizzare i rapporti con i professionisti per la gestione e lo sviluppo delle attività dello studio: collaboratori, dipendenti, i responsabili dei trattamenti, cioè i professionisti esterni che a vario titolo collaborano con lo studio (medici, ecc.), mediante atto di nomina con le istruzioni operative per i trattamenti (art. 29 Reg.to[17]),

---

[16] **Articolo 5** *Principi applicabili al trattamento di dati personali*

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

[17] **Articolo 29** *Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

ovvero contratto che vincoli i responsabili dei trattamenti a specifici obblighi (art. 28 Reg.to[18])

E. Proteggere i pc dalle minacce esterne (tecnico-informatico di fiducia al quale chiedere la soluzione di specifici problemi), salvataggio integrale (back up) di tutti i dati su pc perlomeno 1 volta alla settimana e minimizzare i rischi di perdita accidentale, sottrazione fraudolenta e similari di Pc portatili e altri strumenti informatici rimovibili: ad es., l'uso della penna Usb (premessa l'operatività di una valida password di accesso, è necessario caricare/lasciare nella penna esclusivamente i dati che debbano essere trattati nel

---

[18] **Articolo 28** *Responsabile del trattamento*

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un **contratto** o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

...

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

corso della sessione esterna). Di converso, rottamare nel rispetto della esigenza di protezione dei dati. [19]

F. Sicurezza dello studio, con adozione di misure o cautele atte ragionevolmente a prevenire accessi indesiderati e azioni concretantesi nella lesione della riservatezza, della disponibilità, della integrità delle banche dati.

[19] Si veda il provvedimento del Garante "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008" in G.U. n. 287 del 9 dicembre 2008. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1571514