Il Regolamento Europeo 2016/679/UE

Seminario FIMMG Roma

Roma, 22 Maggio 2018

Il Regolamento in generale

A) LE MISURE DI «RESPONSABILIZZAZIONE» DI TITOLARI E RESPONSABILI (1)

Il regolamento pone con forza l'accento sulla "responsabilizzazione" di titolari e responsabili – ossia, **sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento** (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

A) LE MISURE DI «RESPONSABILIZZAZIONE» DI TITOLARI E RESPONSABILI (2)

Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega **l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano**, come **la notifica preventiva dei trattamenti** all'autorità di controllo e il cosiddetto **prior checking** (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia, con eventuale successiva consultazione dell'Autorità.

B) REGISTRO DEI TRATTAMENTI

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. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

C) MISURE DI SICUREZZA

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, **la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva** ("tra le altre, se del caso"). Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Titolare, responsabile, incaricato del trattamento

Il Regolamento:

1) disciplina **la contitolarità del trattamento** (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;
2) fissa più dettagliatamente (rispetto al Codice) **le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

3) prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti svolti** (ex art. 30, paragrafo 2); l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti (ex art. 32 regolamento); **la designazione di un RPD-DPO** (si segnalano, al riguardo, le linee-guida in materia di responsabili della protezione dei dati adottate dal Gruppo "Articolo 29", disponibili qui anche nella versione in italiano: www.garanteprivacy.it/regolamentoue/rpd), nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che **anche il responsabile** non stabilito nell'Ue dovrà **designare un rappresentante in Italia** quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevedeva l'art. 5, comma 2, del Codice.

4) definisce caratteristiche **soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento).

MODELLO NOMINA INCARICATO AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

Dott. .....
TITOLARE STUTTURA SANITARIA

Il sottoscritto ..... In qualità di titolare del trattamento dei dati della struttura sanitaria ..... con sede in .....

NOMINA QUALE INCARICATO AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

Il signor/a ..... Nato/a a ..... Il .....

In particolare dovrà:

a) *raccogliere, registrare, trattare e conservare i dati personali e sensibili contenuti nelle cartelle cliniche, sia su supporto cartaceo che informatico, avendo cura che l'accesso agli stessi sia consentito solo ai soggetti autorizzati;*
b) *adempiere alla comunicazione dei dati ai soggetti esterni nelle forme previste.*

Le rammento che dovrà adottare la parola chiave riservata per l'accesso alla banca dai elettronica che dovrà esser periodicamente modificata.

Data .....

FIRMA DEL TITOLARE

p.r. Firma dell'incaricato

L’Informativa

A) I CONTENUTI

- I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **deve sempre** specificare **i dati di contatto del RPD-DPO (Responsabile della protezione dei dati-Data Protection Officer),** ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento.
- Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.
- Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

B) LE MODALITA'

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee.

L'informativa è data, **in linea di principio, per iscritto e preferibilmente in formato elettronico**, anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1).

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati** (compreso il diritto alla portabilità dei dati), se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.**

Il Consenso

A) I FONDAMENTI

- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso **deve** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22). Si segnalano, al riguardo, le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy.it/regolamentoue/profilazione.

- **Non** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) **deve** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

- **Il consenso dei minori** è valido **a partire dai 16 anni** (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

- **Deve** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **non** è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

- **Deve** essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

B) I DATI PRECEDENTI

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2).

C) MODELLO RACCOLTA CONSENSO

Il sottoscritto .....nato a.....il..... residente in.....Via.....cap.....Località..... dichiara di essere stato informato su:

1 le finalità e le modalità del trattamento cui sono destinati i dati, connesse con le attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico a tutela della propria salute;

2 i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati (medici sostituti, laboratorio analisi, medici specialisti, farmacisti, aziende ospedaliere, case di cura private e fiscalisti) o che possono venirne a conoscenza in qualità di incaricati;

3 il diritto di accesso ai dati personali, la facoltà di chiederne l'aggiornamento, la rettifica, l'integrazione e la cancellazione nonché di opporsi all'invio di comunicazioni commerciali;

4 il nome del medico che sarà titolare del trattamento dei dati personali nonché l'indirizzo del relativo studio professionale + il nominativo del RDP (Responsabile Protezione Dati);

5 la necessità di fornire dati richiesti per poter ottenere l'erogazione di prestazioni mediche adeguate.

Data

Esprimo il mio consenso al trattamento dei dati personali e sensibili, esclusivamente a fini di diagnosi e cura al Dr.....

Firma dell'interessato

D) MODELLO INFORMATIVA

Gentile Sig./Sig.ra _____(interessato) nato _____il ,residente_____, c.f_____ ai fini previsti dal Regolamento Ue n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, La informo che il trattamento dei dati personali da Lei forniti ed acquisiti dallo Studio _____, saranno oggetto di trattamento nel rispetto della normativa prevista dal premesso Regolamento nel rispetto dei diritti ed obblighi conseguenti e che:

a) FINALITÀ DEL TRATTAMENTO - Il trattamento è finalizzato unicamente alla corretta e completa esecuzione dell'incarico professionale ricevuto sia in ambito giudiziale che extragiudiziale

b) MODALITÀ DEL TRATTAMENTO DEI DATI PERSONALI - Il trattamento è realizzato attraverso operazioni, effettuate con o senza l'ausilio di strumenti elettronici e consiste nella raccolta, registrazione, organizzazione conservazione, consultazione ,elaborazione, modificazione, selezione, estrazione, raffronto utilizzo interconnessione, .blocco, comunicazione cancellazione e distruzione dei dati. Il trattamento è svolto dal titolare e dagli incaricati espressamente autorizzati dal titolare.

c) CONFERIMENTO DEI DATI E RIFIUTO - Il conferimento dei dati personali comuni, sensibili e giudiziari è necessario ai fini dello svolgimento delle attività di cui al punto a) e il rifiuto da parte dell'interessato di conferire i dati personali comporta l'impossibilità di adempiere all'attività di cui al punto a)

d) COMUNICAZIONE DEI DATI - I dati personali possono venire a conoscenza esclusivamente dagli incaricati del trattamento e possono essere comunicati per le finalità di cui al punto a) a collaboratori esterni ,domiciliatari, controparti e loro difensori, ad eventuali arbitri e in generale a tutti i soggetti i quali la comunicazione è necessaria per il corretto espletamento dell'incarico professionale e per le finalità di cui al punto a) I dati personali non sono soggetti a diffusione

e) TRASFERIMENTO DEI DATI ALL'ESTERO - I dati personali possono essere trasferiti verso paesi dell'unione europea o verso paesi terzi rispetto a quelli dell'unione europea o ad un'organizzazione internazionale, nell'ambito delle finalità di cui al punto a). Sarà comunicato all'interessato se esista o meno una decisione de adeguatezza della Commissioone Ue.

f) CONSERVAZIONE DEI DATI - I dati sono conservati per il periodo necessario all'espletamento dell'attività e comunque non superiore a dieci anni

g) TITOLARE DEL TRATTAMENTO - Il titolare del trattamento è l'Avv. …. con studio in ……

h) DIRITTI DELL'INTERESSATO - l'interessato ha diritto :

- all' accesso, rettifica, cancellazione, limitazione e opposizione al trattamento dei dati

- ad ottenere senza impedimenti dal titolare del trattamento i dati in un formato strutturato di uso comune e leggibile da dispositivo automatico per trasmetterli ad un altro titolare del trattamento

- a revocare il consenso al trattamento, senza pregiudizio per la liceità del trattamento basata sul consenso acquisito prima della revoca

- proporre reclamo all'Autorità Garante per la Protezione dei dati personali.

L'esercizio dei premessi diritti può essere esercitato mediante comunicazione scritta da inviare a mezzo pec all'indirizzo o lettera raccomandata a/r all'indirizzo Il/la sottoscritto/a dichiara di aver ricevuto l'informativa che precede. ,

Lì

La nomina del DPO

A) QUANDO LA NOMINA E' OBBLIGATORIA (1)

A mente del Regolamento (art. 37), la nomina del DPO è obbligatoria:

a) a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico, con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali; oppure

b) b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

d) Si tenga presente che la designazione obbligatoria di un DPO può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto comunitario. Inoltre, anche ove il regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29", così come il Garante italiano, incoraggiano un tale approccio "cautelativo".

A) QUANDO LA NOMINA E' OBBLIGATORIA (2)

Nelle ipotesi sub lettere b) e c), che ci occupano, dell'art. 37, paragrafo 1 del Regolamento risulta dirimente, al fine di valutare se sussista o meno l'obbligo di nomina di un DPO, è che il trattamento avvenga su "larga scala".

Il Regolamento non fornisce una definizione di "trattamento su larga scala", anche se il considerando 91 fornisce indicazioni in proposito, ricomprendendovi, in particolare, "trattamenti... 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".

B) IL MONITORAGGIO REGOLARE E SISTEMATICO

Anche il concetto di "monitoraggio regolare e sistematico degli interessati" non trova definizione nel Regolamento; a mente del considerando 24, vi rientra certamente ogni forma di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

Le linee guida forniscono anche alcune utili esemplificazioni di attività di monitoraggio sistematico e regolare, tra le quali: il curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; i programmi di fidelizzazione; l'utilizzo di telecamere a circuito chiuso; i dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica.

Anche sotto tale profilo, sembra escludersi l'obbligo della nomina del DPO per lo studio medico.
E' previsto, invece, il conferimento dell'incarico, in forma scritta, a collaboratori, segretari e consulenti, come da modello allegato

Le sanzioni

A) ARTICOLO 82

Diritto al risarcimento e responsabilità

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.