DoctorNews del 25 maggio 2018

“Entra in vigore oggi la normativa europea sulla protezione dati, in sigla Gdpr (General Data Protection Regulation). Riguarda tutta la filiera che accompagna i dati personali di ciascuno, coinvolgendo quindi aziende, pubblica amministrazione, e professionisti. Il GDPR si basa, infatti, sul principio di "responsabilizzazione" di chiunque effettui operazioni di trattamento nell'ambito della propria attività (il cosiddetto "titolare del trattamento"). Significa, quindi, che ciascuno dovrà fare le valutazioni e le scelte adatte alla propria specifica realtà. E le sanzioni per l'inosservanza delle norme possono arrivare fino a 20 milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale. Il Regolamento è destinato ad abrogare la Direttiva 95/46 che ha portato l'Italia all'adozione dell'attuale Codice Privacy (il Decreto Legislativo n. 196/2003), norme che sono state adottate però in un contesto tecnologico completamente diverso, prima cioè che internet, social media, cloud e servizi in rete cambiassero definitivamente il modo di vivere e lavorare. Ora, le nuove norme mirano proprio ad adeguare il livello di protezione dei dati all'evoluzione degli strumenti che si utilizzano quotidianamente e con cui si registrano, trasmettono e archiviano i dati di utenti e dipendenti. L'Italia sta lavorando a un decreto legislativo con l'obiettivo di adeguare le norme italiane al Gdpr che troverà comunque applicazione a prescindere dall'adozione del decreto entro due giorni. Pertanto niente proroghe o differimenti. Ecco una guida, con le novità principali che il Gdpr introduce.

Data protection officer

Il Regolamento prevede l'obbligo per alcuni soggetti di nominare un Dpo - Data Protection Officer (ovvero il responsabile della protezione dei dati personali). Si tratta di una figura, interna o esterna alla struttura del titolare, che deve possedere dei requisiti specifici (ad esempio in termini di esperienza e competenza) e deve occuparsi della corretta applicazione della normativa, curando con particolare attenzione la formazione del personale. Il Dpo è obbligatorio quando il trattamento è effettuato da una pubblica amministrazione (eccezion fatta per le autorità giurisdizionali) e quando le attività di trattamento consistano nel monitoraggio su larga scala degli interessati oppure determinino il trattamento su larga scala di dati sensibili (dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, 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). Il Garante Privacy ha chiarito che, anche quando non obbligatoria, la nomina del Dpo è comunque sempre consigliata in quanto può rappresentare un valido supporto.

Valutazione d'impatto e registro dei trattamenti

Nel caso in cui i trattamenti posti in essere siano particolarmente rischiosi per i diritti e le libertà degli interessati (ad esempio, la videosorveglianza), il titolare è obbligato a una valutazione preliminare di impatto sulla tutela dei dati (cosiddetta "privacy impact assessment"), con una precisa analisi dei rischi e delle contromisure poste in essere. Inoltre, tutte le organizzazioni con più di 250 dipendenti oppure che - indipendentemente dal numero dei dipendenti - pongano in essere trattamenti potenzialmente pericolosi sono tenute all'adozione di un "registro delle attività di trattamento" che contenga, tra le altre informazioni, la descrizione delle misure di sicurezza adottate.

Informativa e consenso

Gli utenti devono essere informati in modo semplice e chiaro sulle finalità, modalità e ambito del trattamento. Le informative richieste agli utenti (dal form per una newsletter ai moduli per

richiedere una fidelity card) devono quindi essere aggiornate, prevedendo alcune informazioni nuove (come la base giuridica del trattamento e il tempo di conservazione dei dati) e semplificando il testo in modo da renderle realmente comprensibili. Particolare attenzione è dedicata alla tutela dei minori che - per accedere ai servizi della società dell'informazione (come i social network) - devono avere almeno 16 anni per poter prestare autonomamente il consenso al trattamento.

Sicurezza

Ogni titolare del trattamento è tenuto ad adottare misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati. Non esiste un elenco di misure di sicurezza "minime" uguali per tutti. Spetta a ciascuno decidere e assumersi le responsabilità di quali siano le contromisure adeguate alla propria realtà (crittografia, controllo degli accessi, sorveglianza degli archivi, ecc.).

Data Breach

Viene introdotto il diritto degli interessati di venire a conoscenza delle violazioni dei propri dati personali ("data breach"). Questo significa che - nel caso di incidenti di sicurezza relativi ai sistemi utilizzati per il trattamento (come lo smarrimento di una chiavetta Usb, il furto di un fascicolo oppure un attacco informatico) - il titolare del trattamento dovrà organizzarsi per procedere alla notificazione al Garante Privacy senza ritardo (e, comunque entro le 72 ore). Inoltre, la comunicazione dovrà essere data a tutti gli interessati, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (ipotesi assai probabile, ad esempio, nel caso dei dati sanitari o dei servizi di posta elettronica o messaggistica).

Sanzioni

Il sistema sanzionatorio previsto del Gdpr è molto più severo rispetto a quello del Codice Privacy. Le sanzioni amministrative - che saranno inflitte dal Garante Privacy - possono arrivare fino a 20 milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale. In attesa di vedere se e quali saranno gli illeciti penalmente rilevanti previsti dal Decreto che il governo italiano si appresta ad adottare, è importante tenere a mente che chiunque subisca un danno da una violazione del Gdpr ha il diritto di ottenerne il risarcimento dal titolare, a meno che quest'ultimo non dimostri che il danno non gli è alcun modo imputabile".

Quotidiano Sanità del 25.05.2018

Il nuovo regolamento europeo in materia di protezione dei dati personali (Gdpr), entrato in vigore il 25 maggio 2016, si applica in tutti gli Stati Membri a partire da oggi, 25 maggio 2018. Il Regolamento intende dare vita ad un quadro più solido e coerente in materia di privacy, affiancato da efficaci misure di attuazione e rafforzare la certezza giuridica e operativa tanto per le persone fisiche quanto per gli operatori economici che per le autorità pubbliche.

Il Regolamento UE si articola in 11 capi per un totale di 99 articoli. Ai fini dell'adeguamento della disciplina italiana nelle materie oggetto del Regolamento il Governo Gentiloni ha varato un apposito decreto legislativo che è stato trasmesso per i pareri alle Commissioni speciali di Camera e Senato o scorso 10 maggio (vedi altro articolo).

Per quanto riguarda la sanità il decreto legislativo se ne occupa all'**articolo 6** dello che detta disposizioni specifiche per il **trattamento dei dati personali in ambito sanitario**, intervenendo sugli articoli da 75 a 94 del Codice della privacy. Innanzitutto, nel Capo I, relativo ai principi generali, con la modifica dell'articolo 75, la riforma delinea la cornice di liceità del trattamento dati effettuato per finalità di **tutela della salute** e dell'incolumità fisica dell'interessato, di terzi o della collettività, richiamando le pertinenti disposizioni del Regolamento UE e della parte generale del Codice.

Tale trattamento può riguardare dati particolari (es. origine razziale o etnica, convinzioni religiose, 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) purché:

- **trattamento sia necessario per finalità di medicina** preventiva o di medicina del lavoro, di valutazione della capacità lavorativa del dipendente, di 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 (art. 9, par. 2, lett. h) del Regolamento UE). Tale professionista deve essere soggetto al segreto professionale (art. 9, par. 3, del regolamento UE);
- **il trattamento sia 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 (art. 9, par. 2, lett. i) del Regolamento UE).

Quando ricorrono queste condizioni **il consenso dell'interessato non è richiesto.**

Il trattamento dati in ambito sanitario, inoltre, deve rispettare le **misure di garanzia** per i dati genetici, biometrici e relativi alla salute. In base a tale disposizione, spetta al Garante adottare misure di garanzia ed eventualmente ulteriori condizioni sulla base delle quali il trattamento è consentito. Questa possibilità è offerta agli Stati dall'art. 9, par. 4, del Regolamento UE che, per questi dati – oltre che per i dati biometrici e genetici – consente di mantenere o introdurre ulteriori condizioni e limitazioni. Dalla lettura dell'art. 2-septies, comma 6, che consente al Garante in relazione ai dati genetici ed ai dati sanitari, diagnostici e relativi alle prescrizioni di medicinali di "individuare in caso di particolare ed elevato livello di rischio, **il consenso come ulteriore misura di protezione dei diritti dell'interessato**", si desume che il Garante potrà reintrodurre il consenso per il trattamento di alcuni specifici dati relativi alla salute e per i dati genetici.

In presenza di questi presupposti e requisiti il trattamento dati è lecito e, in base al nuovo comma 2 dell'articolo 75, l'interessato non può esercitare il diritto all'oblio (articolo 17 del Regolamento) e il diritto alla portabilità dei dati (articolo 20 del Regolamento). Tali **limitazioni ai diritti** sono espressamente fondate sull'articolo 23 del Regolamento che le consente per salvaguardare la sanità pubblica (par. 1, lett. e).

Coerentemente con l'eliminazione del requisito del consenso, la riforma **abroga l'articolo 76 del Codice** che distingue, per la sanità pubblica, i trattamenti dati che possono essere effettuati anche senza il consenso dell'interessato, ma previa autorizzazione da parte del Garante, da quelli che necessitano del consenso.

Il Capo II è dedicato alle modalità particolari per informare l'interessato del trattamento dati e per trattare i dati stessi. Si tratta di **disposizioni che dovranno applicare tutti gli esercenti professioni sanitarie e le strutture sanitarie e socio-sanitarie** tanto pubbliche quanto private, nonché gli altri soggetti pubblici operanti in ambito sanitario o della protezione e sicurezza sociale in base all'art. 80 del Codice. Tutti questi soggetti dovranno, anzitutto, informare l'interessato del trattamento dati.

Anche dall'**articolo 77 è eliminato ogni riferimento al consenso dell'interessato.**

L'articolo 78, relativo alle **informazioni che devono rendere il medico di medicina generale o il pediatra**, è coordinato con la modifica dell'articolo 77, e dunque con il rinvio alle informazioni previste dagli articoli 13 e 14 del Regolamento, che questi medici potranno rendere con **un'unica informativa**, relativa al complesso del rapporto medico/paziente che si protrarrà nel tempo.

È inoltre integrato l'elenco dei trattamenti rispetto ai quali le informazioni devono evidenziare specifici rischi per i diritti e le libertà fondamentali: alla ricerca scientifica, alla teleassistenza o telemedicina ed ai servizi resi attraverso la comunicazione elettronica si aggiungono ora il **fascicolo sanitario elettronico e i sistemi di sorveglianza ed i registri nel settore sanitario** (disciplinati dall'art. 12 del decreto-legge n. 179 del 2012).

Il **fascicolo sanitario elettronico (FSE)** è l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito. Il FSE – che deve consentire anche l'accesso da parte del cittadino ai servizi sanitari on line - è istituito dalle regioni e province autonome, a fini di prevenzione, diagnosi, cura e riabilitazione; studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria. Al fascicolo sanitario elettronico si accompagna il **dossier farmaceutico**, aggiornato a cura della farmacia che effettua la dispensazione.

I **sistemi di sorveglianza e i registri di mortalità, di tumori e di altre patologie**, di trattamenti costituiti da trapianti di cellule e tessuti e trattamenti a base di medicinali per terapie avanzate o prodotti di ingegneria tessutale e di impianti protesici sono istituiti ai fini di prevenzione, diagnosi, cura e riabilitazione, programmazione sanitaria, verifica della qualità delle cure, valutazione dell'assistenza sanitaria e di ricerca scientifica in ambito medico, biomedico ed epidemiologico allo scopo di garantire un sistema attivo di raccolta sistematica di dati anagrafici, sanitari ed epidemiologici per registrare e caratterizzare tutti i casi di rischio per la salute, di una particolare malattia o di una condizione di salute rilevante in una popolazione definita.

Con queste due integrazioni all'*articolo 78*, lo schema di decreto legislativo può procedere all'abrogazione degli articoli 91 e 94 del Codice, rispettivamente relativi ai dati trattati mediante carte e ai registri in ambito sanitario.

Finalità di coordinamento normativo hanno anche le modifiche all'**articolo 79** del Codice, in relazione alle informazioni che devono rendere le strutture sanitarie pubbliche e private, e all'**articolo 80** del Codice, in relazione agli altri soggetti pubblici operanti in ambito sanitario o della protezione e sicurezza sociale: anche queste strutture potranno utilizzare **un'unica informativa**, in riferimento a una pluralità di prestazioni erogate da distinti reparti o articolazioni della struttura.

L'**articolo 81** del Codice, relativo alla **prestazione del consenso**, è **abrogato**.

L'**articolo 82**, relativo alla possibilità di rendere le informazioni sul trattamento dati successivamente all'erogazione della prestazione sanitaria – in presenza di una emergenza – è coordinato con la previsione delle informazioni di cui agli articoli 13 e 14 del Regolamento ed è integrato, quanto alla possibilità di rendere le informazioni ai congiunti, da un richiamo alle **unioni civili** (legge n. 86 del 2016) e al fiduciario disciplinato nell'ambito delle **disposizioni anticipate di trattamento** (legge n. 219 del 2017, art. 4).

Gli **articoli 83 e 84**, che specificano alcune cautele a tutela della privacy da osservare da parte degli organismi sanitari e degli esercenti professioni sanitarie nell'**organizzazione delle prestazioni e dei servizi**, nonché nella **comunicazione di diagnosi o referti** all'interessato, sono **abrogati**. In merito interviene ora l'articolo 2-septies del Codice, che individua misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute e che prescrive al Garante, nel provvedimento che ogni due anni delinea le misure di garanzia, di individuare anche cautele relativamente a "b) profili organizzativi e gestionali in ambito sanitario; c) modalità di comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute" (comma 4).

Il Capo III del titolo dedicato ai trattamenti in ambito sanitario, composto dagli **articoli 85 e 86** del Codice, che attribuiscono la **qualifica di rilevante interesse pubblico** a una serie di attività del Servizio sanitario nazionale e alle attività amministrative inerenti a maternità, tossicodipendenze e handicap, è **abrogato**. Le corrispondenti qualificazioni sono sostanzialmente contenute ora nell'articolo 2-sexies del Codice, con particolare riferimento alle lettere q), r) ed s).

La riforma **abroga** gli **articoli 87, 88 e 89 del Codice**, che disciplinano le **prescrizioni mediche**. Viene infatti inserito un **nuovo articolo 89-bis**, per disciplinare il caso in cui la **prescrizione di medicinali non richieda l'inserimento del nominativo** dell'interessato. In tal caso si rinvia comunque alle cautele particolari che dovrà dettare il Garante nell'ambito del provvedimento contenente le misure di garanzia in base all'articolo 2- septies.

La riforma **abroga** il Capo V, composto dal solo **articolo 90**, relativo ai **dati genetici**. Si tratta della disposizione che oggi consente il trattamento di tali dati solo previa autorizzazione rilasciata dal Garante sentito il Ministro della salute e con il parere del Consiglio superiore di sanità.

A seguito dell'abrogazione, si applica il Regolamento UE, che anzitutto definisce i dati genetici come "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". Si tratta di **dati personali particolari** (art. 9 del Regolamento) che possono essere trattati solo con il **consenso espresso dell'interessato** ovvero se ricorrono altri presupposti di liceità espressamente elencati dall'art. 9, par. 2, del regolamento (come, ad esempio, esigenze di diagnosi in ambito sanitario). Inoltre, in base al par. 4 dell'art. 9 "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".

In merito, interviene l'articolo 2-septies del Codice che, fermo il divieto di diffusione dei dati genetici, consente al Garante di dettare – per i dati genetici e sanitari - misure di garanzia, sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanità, che possono spingersi fino a **prevedere il consenso come ulteriore misura di protezione dei diritti dell'interessato** (comma 6).

Infine, quanto al Capo VI, che reca disposizioni varie, la riforma:

- **abroga l'articolo 91**, sui dati trattati mediante carte anche non elettroniche. L'abrogazione è compensata dall'introduzione del richiamo dal fascicolo sanitario elettronico all'articolo 78;
- apporta limitati interventi di **coordinamento** all'**articolo 92**, sulle cartelle cliniche;
- non modifica l'articolo 93 sul certificato di assistenza al parto;
- **abroga l'articolo 94**, su banche dati, registri e schedari in ambito sanitario. Anche questa abrogazione è compensata dall'inserimento nell'articolo 78 di un riferimento ai sistemi di sorveglianza ed ai registri di cui all'art. 12 del decreto-legge n. 179 del 2012.

In relazione al trattamento dati in ambito sanitario, il nuovo articolo 166 del Codice, sanziona la violazione degli obblighi di tenuta delle cartelle cliniche (art. 92) e di redazione del certificato di assistenza al parto con la possibile applicazione della **sanzione amministrativa pecuniaria fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.**