**Riapertura** **Sanit?** 31 LUGLIO 2017

GDPR/ Cosa cambia con l'applicazione del Regolamento 2016/679 a partire dal 25 maggio 2018

# Privacy&sanità, la Ue fissa i paletti


Manca ormai meno di un anno all'applicazione del Regolamento Ue 2016/679: entro il 25 maggio 2018, tutte le imprese private e gli organismi pubblici dovranno adeguarsi alla nuova normativa europea in materia di protezione dei dati personali.

Come noto, infatti, il Regolamento ha efficacia applicativa diretta nell'ordinamento di ciascuno Stato membro, senza necessità di formale recepimento o dell'emanazione di una normativa di attuazione.

In ambito sanitario, molte realtà rilevanti a livello nazionale come ospedali e centri di ricerca hanno già avviato percorsi strutturati di allineamento alla normativa europea, sia sulla scorta di una maggiore sensibilità sviluppata sotto la previgente disciplina (il Garante ha spesso focalizzato parte della propria attività di vigilanza su tali strutture) sia per la sfida impegnativa che il principio di accountability pone, sotto il profilo organizzativo e tecnologico, nonché per le possibili conseguenze sanzionatorie. La sfida maggiore nell'attività di compliance al Gdpr attende, comunque, le strutture sanitarie di media o piccola dimensione, dove il cambio generale di approccio alla gestione della privacy coinvolgerà maggiormente il management e, in particolare, il Titolare, nella scelta del più corretto percorso di allineamento, che dovrà essere basato su soluzioni confezionate su misura, e non su schemi e documentazione standard.

**Il trattamento dei dati sanitari nel Gdpr.** La declinazione delle norme del Gdpr nel settore sanitario deve considerare necessariamente alcune implicazioni, prime tra tutte, quelle connesse alle disposizioni di carattere definitorio dedicate ai «dati genetici» (articolo 4, n. 13) e ai «dati biometrici» (artioclo 4, n. 14), nonché ai «dati relativi alla salute» (articolo 4, n. 15). Nel quadro della normativa attualmente vigente, tali dati sono ricondotti alla categoria dei sensibili; le definizioni del Regolamento saranno, invece, decisive nell'individuazione e corretta attuazione delle norme che prevedono casi di trattamento legittimo, anche in assenza del consenso dell'interessato, connessi alle finalità di medicina preventiva o del lavoro, alla valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero alla gestione dei sistemi e servizi sanitari o sociali, nonchè ai motivi di interesse pubblico nel settore della sanità pubblica.

Tra i molteplici nuovi adempimenti, il Gdpr prevede, inoltre, al verificarsi di talune circostanze, la designazione del Responsabile della protezione dei dati (Rpd), meglio conosciuto come Data protection officer (Dpo).

Il Dpo deve essere designato obbligatoriamente da tutte le autorità pubbliche e da tutti gli organismi pubblici (così come definiti dall'articolo 3 del Dlgs 50/2016), nonché da tutti quei soggetti privati che, come attività principale, effettuano un monitoraggio regolare, sistematico e su larga scala delle persone fisiche ovvero trattano su larga scala categorie particolari di dati.

La nomina obbligatoria del Dpo in ambito sanitario è stata confermata dalle «Linee-guida sui responsabili della protezione dei dati (Rpd)», adottate dal Gruppo di Lavoro Articolo 29 il 13 dicembre 2016 (nella versione emendata in data 5 aprile 2017), ove è stato chiarito che l'espressione «attività principali» non escludere quei casi in cui il trattamento dei dati costituisce comunque una componente inscindibile dalle attività svolte dal titolare. A tale riguardo, viene introdotto l'esempio di un ospedale dove l'attività principale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute.

Altro tema importante da considerare in ambito sanitario è quello introdotto dall'articolo 9, comma 4, del Gdpr secondo il quale «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», ammettendo, pertanto, spazi di intervento locali che presuppongono un apporto legislativo specialistico.

L'applicazione del Gdpr a livello locale non potrà, peraltro, prescindere dalle leggi speciali in materia sanitaria, attraverso un equo bilanciamento degli interessi in gioco. Si pensi ad esempio, al diritto dell'interessato, e quindi del paziente, alla cancellazione dei dati (articolo 17), che dovrà necessariamente tenere conto, come in più occasioni affermato dallo stesso

Garante, degli obblighi di conservazione per un tempo illimitato della cartella clinica (articolo 17, comma 3, lettera c).

Un altro esempio è costituito dal diritto alla portabilità dei dati (articolo 20) e dal coordinamento con il tema della trasparenza della documentazione sanitaria, introdotto dall'articolo 4 della legge 24/2017, sulla base del quale la direzione sanitaria della struttura pubblica o privata fornisce la documentazione disponibile, relativa al paziente, preferibilmente in formato elettronico, entro sette giorni dalla presentazione della richiesta da parte degli interessati aventi diritto.

**CLAUDIA GRILLI** Deloitte legal 

**Principali punti di impatto del Gdpr in ambito sanitario**

| | |
|---|---|
| **Designazione del Data protection officer** | Il Dpo deve essere designato obbligatoriamente da tutte le autorità pubbliche e da tutti gli organismi pubblici nonché da tutti quei soggetti privati che, come attività principale, effettuano un monitoraggio regolare, sistematico e su larga scala delle persone fisiche ovvero trattano su larga scala categorie particolari di dati (cfr. «Linee-guida sui responsabili della protezione dei dati (Rpd)», adottate dal Gruppo di Lavoro Articolo 29) |
| **Dati biometrici** | «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» |
| **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» |
| **Dati relativi alla salute** | «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» |

**Spunti di riflessione**

| | |
|---|---|
| **Ricerca scientifica** | Il Regolamento si pone in una posizione di continuità rispetto alla direttiva 95/47/Ce in materia di ricerca scientifica. Viene proposta una ampia accezione del termine ricerca scientifica, includendosi a titolo esemplificativo lo «sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati». Vengono previste inoltre particolari limitazioni per l'esercizio dei diritti degli interessati con specifico riferimento al trattamento di dati per fini di ricerca scientifica |
| **Cartelle cliniche** | Il diritto dell'interessato alla cancellazione dei dati (articolo 17), dovrà necessariamente tenere conto degli obblighi di conservazione illimitati della cartella clinica |
| **Diritto alla portabilità** | Il diritto alla portabilità dei dati potrà essere letto in coordinamento con il tema della trasparenza della documentazione sanitaria, introdotto dall'articlo 4 della legge 24/2017 |

*Fonte: Deloitte legal*