Ordine dei Medici Chirurghi e degli Odontoiatri della provincia di Trento

Trento, 28 giugno 2018

prot. n. 2938-0109

LE FAQ SUL NUOVO REGOLAMENTO UE 679/2016 SUL TRATTAMENTO DEI DATI PERSONALI

Dal 25 maggio 2018 è applicabile il Regolamento UE sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e libera circolazione di tali dati, è una norma direttamente vigente in tutti gli stati europei.

Il Parlamento italiano ha tempo sino al 23 agosto 2018 per armonizzare l'attuale Codice Privacy al Regolamento UE che è fonte però prevalente.

Alla categoria dei medici ed odontoiatri si applica la nuova normativa?

Il Regolamento si applica a tutti i soggetti pubblici e privati che trattano dati personali di persone fisiche, sia di natura comune che sensibile, contenuti sia su archivi cartacei sia su archivi informatici.

Ne sono quindi interessate sia le struttura sanitarie mediche pubbliche e private sia gli studi professionali in qualunque forma organizzati.

Che impatto avrà sulla professione del medico?

Il Regolamento introduce di nuove regole organizzative e di sistema per il corretto trattamento dei dati personali. Fondamentalmente la protezione dei dati delle persone non sarà più un adempimento formale ma inciderà sostanzialmente sulla organizzazione delle strutture, ponendo con forza l'accento sulla responsabilizzazione dei Titolari del trattamento e sulla necessità sin dall'inizio di fare un'analisi preventiva dei rischi e un impegno applicativo specifico e dimostrabile. La Federazione Nazionale degli Ordini dei Medici, comunque nel breve, dovrebbe mettere a disposizione informazioni utili circa la concreta applicabilità della norma agli iscritti.

Ma cosa cambia e quali misure si devono mettere in atto ?
In pillole: alcuni adeguamenti sono necessari alle **informative** e **consensi.** Il Regolamento ci conferma che ogni trattamento deve essere fondato in un'idonea base giuridica (consenso, adempimento obblighi contrattuali, o di legge a cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interessi vitali della persona interessata o di terzi, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Il **consenso** per i dati i dati relativi allo stato di salute deve essere **esplicito**, quindi non occorre sia dato in forma scritta, ma il Titolare del trattamento nel caso in cui questo fosse fondato sul consenso, deve essere in grado di dimostrarlo. Il consenso in ogni caso dovrà essere libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto. Le novità rispetto alle **informative** art. 13 e 14 del Regolamento sono sostanzialmente la necessità di specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione e l'indicazione dei nuovi diritti dell'interessato, quale ad esempio il diritto di presentare un reclamo all'autorità di controllo.
L'informativa dovrà contenere anche i dati di contatto del **DPO**, Data Protection Officer, nel caso fosse nominato dal Titolare. La nomina di questa nuova figura professionale è obbligatoria per i soggetti pubblici ma anche, tra gli altri, **per tutti i soggetti la cui attività principale consiste in trattamenti in su larga scala di categorie particolari di dati personali**. Le uniche indicazioni oggi per gli studi medici è che la nomina non sia obbligatoria per le attività dei liberi professionisti che liberi professionisti operanti in forma individuale; anche se la nomina di un DPO (o Responsabile Protezione Dati in italiano) è dallo stesso Garante consigliata vivamente per supportare il titolare nell'adempimento degli obblighi sulla privacy.
Il DPO è un professionista che deve essere in possesso di adeguata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali e ha il compito di aiutare le organizzazioni in cui opera a mantenersi conformi alle nuove regole sulla protezione della privacy e a sensibilizzare e formare il personale. Il DPO funge da punto di contatto per tutte le richieste degli interessati e anche da intermediario con le autorità di controllo, in particolare l'autorità giudiziaria, il Garante della Privacy e la Guardia di Finanza.

Altra importante novità è la necessità di dotarsi all'interno delle proprie strutture dei **registri dei trattamenti e delle violazioni** che sono uno strumento fondamentale per avere un quadro aggiornato dei trattamenti in essere all'interno e nel caso di controlli dell'Autorità. Così l'attenzione che il regolamento dà alla **formazione del personale** che deve essere adeguatamente istruito sulle procedure degli studi in materia di privacy.

Quanto alle **sanzioni** il titolare del trattamento risponde personalmente delle violazioni commesse in quanto è suo dovere rispettare la normativa e proteggere con l'adozione di misure organizzative e tecniche adeguate alla propria realtà professionale, i dati dei propri pazienti. Mentre il DPO non risponde delle sanzioni ma ovviamente risponde rispetto al suo incarico professionale.

Consigli operativi

In questo momento ci riteniamo di consigliare un piano di lavoro concreto che implichi:

- Lo svolgimento dell'attività di **valutazione della obbligatorietà/opportunità** di designazione del DPO
- **La mappatura** dati, banche dati, ti trattamenti, finalità interessati e destinatari ;
- Esaminare e **adeguare informative e consensi**
- **Redigere il registro dei trattamenti**
- Redigere una procedura per le risposte **all'esercizio dei diritti** degli interessati
- Effettuare una **analisi dei rischi** (organizzativi, fisici sanzionatori, informatici) e predisporre le misure minime adeguate alla propria struttura
- Redigere un **organigramma** privacy nelle strutture più complesse
- Rivedere gli **incarichi** soprattutto dei responsabili del trattamento
- Revisione dei contratti fornitori informatici e di dati(servizi cloud)
- **Effettuare attività di formazione** generale e degli incaricati/autorizzati
- Predisporre un **piano di sicurezza** anche al fine della comunicazione di data breach
- **Rendicontare** il percorso di adeguamento
- **Verificare e aggiornare** periodicamente le procedure.

Nella speranza dato qualche utile informazione per orientarsi nella materia , in attesa di fornirmi maggiori elementi utili.

Ordine dei Medici Chirurghi e degli Odontoiatri della provincia di Trento