Prot.488/2018

Le Novità introdotte dal GDPR (Regolamento EU Privacy)

Il 25 maggio 2018 entra in vigore il Regolamento Europeo sulla privacy, che introduce molteplici novità in materia di tutela della Riservatezza;

in modo particolare, viene stabilito il principio della "**Responsabilizzazione**" (*Accountability*) che prevede l'obbligo da parte del **Titolare** del Trattamento Dati Personali di dimostrare l'adeguatezza delle misure adottate nel tutelare la riservatezza e la protezione dei dati personali degli **interessati** (i pazienti).

Di conseguenza, il principio della Responsabilizzazione impone un approccio basato sulla valutazione dei rischi associati al Trattamento dei Dati personali, con l'introduzioni di nuovi adempimenti in capo a Titolari e Responsabili del Trattamento tra cui la **valutazione di impatto (DPIA)**, la tenuta del **Registro dei Trattamenti** nei casi previsti dalla normativa, l'adozione di **misure di sicurezza adeguate (**anziché **minime** come in precedenza), l'eventuale nomina del **Responsabile della Protezione Dati (RDP-DPO)**.

Il principio della Responsabilizzazione impone quindi una valutazione **caso per caso** della adeguatezza delle misure adottate dai singoli Titolari del Trattamento;

le linee guida che vengono di seguito riportate hanno pertanto valore esemplificativo e non esaustivo.

I Soggetti del GDPR

La normativa europea ha modificato i ruoli e i soggetti già previsti in precedenza dal Testo Unico sulla Privacy, introducendone dei nuovi o aggiornando le norme previste per i precedenti ruoli;

di seguito si descrive sinteticamente il quadro attuale dei soggetti e delle relative responsabilità:

Titolare del Trattamento: Tale ruolo è normalmente ricoperto dal Titolare dello Studio Medico ma il GDPR disciplina anche la **contitolarità del trattamento** *(art. 26)* e impone ai titolari di definire specificamente (con un atto giuridico) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati (i pazienti)**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

- **Responsabile del Trattamento:** E' designato dal Titolare per lo svolgimento di **specifici compiti** nell'ambito del trattamento dei dati (ad es. la tenuta della contabilità); il GDPR 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; l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti; la **designazione di un RPD-DPO** nei casi previsti dal regolamento o dal diritto nazionale;
- **Incaricati del Trattamento:** Pur non prevedendo più espressamente la **figura dell' "incaricato" del trattamento**, il GDPR **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";
- **Responsabile Protezione Dati (RDP-DPO):** Il **Responsabile della Protezione dei Dati Personali** (**RPD-DPO**) è la nuova figura introdotta dal GDPR; viene **designato** dal Titolare dello studio medico, e ha il compito di verificare la conformità del trattamento dei dati alle regole previste dalla normativa sulla tutela della riservatezza; il **RPD-DPO** funge da intermediario tra lo studio e l'autorità di controllo (Garante della Privacy), e le sue attività consistono nel **monitoraggio sistematico** dell'adeguatezza del trattamenti dei dati personali, nonché dei sistemi utilizzati per la loro protezione, anche al fine di prevenire eventuali **"Data Breaches"**. **Attenzione:** malgrado venga impropriamente denominato come "*Responsabile* della Protezione Dati", in realtà il **RDP-DPO** assume una funzione **consultiva,** e gli **unici reali responsabili** per il rispetto delle norme di legge rimangono il **Titolare** del Trattamento e il **Responsabile** del Trattamento.

- **Interessati del Trattamento:** Sono comunemente i pazienti, ma possono anche essere altre persone fisiche in relazione alle quali vengono raccolti e trattati i dati personali.

Le principali prescrizioni del GDPR per i Medici

Informativa e Consenso: il GDPR si ispira al principio di trasparenza il quale impone che le informazioni destinate all'interessato siano facilmente accessibili e di facile comprensione e che sia utilizzato un **linguaggio semplice e chiaro**; il GDPR, in linea con il passato, prevede che il consenso al trattamento sia informato e specifico e che venga prestato liberamente dall'interessato. In modo particolare occorre prestare attenzione alle seguenti prescrizioni:

- L'informativa deve essere fornita all'interessato **prima di effettuare la raccolta dei dati e deve essere fornita in relazione ai diversi trattamenti posti in essere (non è possibile quindi fornire una "Informativa generale");** è inoltre opportuno che i titolari del trattamento **verifichino la rispondenza delle informative** attualmente utilizzate alle nuove norme, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento;
- il titolare **DEVE SEMPRE** specificare i **dati di contatto del RPD-DPO** ove esistente;
- 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 ("profilazione") l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato;
- l'informativa 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; il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione"**

con l'informativa estesa; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

Tenuta del Registro delle Attività di Trattamento: Il GDPR introduce l'obbligo di tenuta del Registro delle Attività; si tratta di **un registro dove vengono rendicontate le attività svolte sui dati dei pazienti**,

La tenuta del Registro delle Attività è **obbligatoria** nei seguenti casi (art. 30 GDPR):

- Aziende o Organizzazioni con **più di 250 dipendenti**;
- **In ogni caso,** qualora il trattamento possa presentare un rischio per i diritti e le libertà dell'interessato, ovvero il trattamento non sia occasionale o abbia ad oggetto il trattamento di categorie particolari di dati previsti dall'art. 9 GDPR, quali **dati genetici, dati biometrici, o relativi alla salute;**

Il GDPR prevede che l'obbligo della tenuta del Registro delle Attività ricada direttamente **sul Titolare** del trattamento; tuttavia, le linee guida elaborate dal Gruppo di Lavoro della Commissione Europea (WP29) sostengono che è prassi comune affidare questo compito al **RPD-DPO**, qualora se ne sia nominato uno.

Nomina del Responsabile Protezione Dati (RDP-DPO): La **nomina del RPD-DPO è obbligatoria per tutte le autorità pubbliche** (comprese le Aziende Sanitarie Locali) nonché per **le attività il cui esercizio comporta la manipolazione di dati in larga scala** per speciali categorie di dati, tra i quali i dati sanitari.

Il GDPR non specifica la misura o la quantità di dati definita "larga scala" e al momento la stessa Commissione Europea, nonché il Garante della Privacy, sono discordanti in merito all'obbligatorietà della nomina del RPD-DPO per gli studi medici.

Secondo il *Considerando 91*, infatti, gli studi medici, odontoiatrici e professionali con **un solo Titolare** del trattamento dei dati personali dei pazienti **non sono obbligati** a nominare un RPD-DPO.

Tuttavia, se lo studio medico è **convenzionato con il SSN**, il Garante della Privacy raccomanda fortemente di nominare un **RPD-DPO**.

La Valutazione di Impatto (DPIA): Essendo ispirato al principio della valutazione del rischio, il GDPR prevede una particolare procedura (la DPIA, Data Protection Impact Assessment) da **porre in essere ed aggiornare sistematicamente**, volta ad individuare i possibili rischi legati al trattamento dei dati personali. Tale valutazione di impatto presuppone l'acquisizione di competenze specialistiche in ambito di gestione dei rischi ed è pertanto opportuno che venga condotta da figure professionali specializzate.