

**PRIVACY – PROTEZIONE DEI DATI PERSONALI**  
**GDPR (General Data Protection Regulation-Regolamento UE 2016/679)**  
**Entrata in vigore: 25\05\18**

A seguito di numerosissime richieste da parte degli iscritti, si evidenzia che sono tenuti alla designazione del Responsabile della protezione dei dati personali (RPD o DPO, secondo l'acronimo inglese Data Protection Officer), oltre ai soggetti pubblici, anche i soggetti privati, le cui principali attività implicino il trattamento di dati personali c.d. “comuni” o “sensibili”.

A titolo esemplificativo, nella categoria dei “soggetti privati”, rientrano le società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione e di diagnostica.

Viceversa, non sono obbligati alla designazione del DPO, ad esempio, i liberi professionisti operanti in forma individuale.

In tale ultima ipotesi, la designazione in questione è “raccomandata” (e, quindi, si ribadisce, non vi è alcun vincolo).

Naturalmente, anche i liberi professionisti operanti in forma individuale (come già in precedenza), anche alla luce del GDPR, restano obbligati al pieno rispetto della normativa in tema di protezione dei dati personali dei propri clienti.

In proposito, si segnala che, sul sito del Garante per la Privacy (<http://www.garanteprivacy.it>) sono presenti numerosi documenti utili per approfondimenti pratici sul tema; fra questi segnaliamo, oltre al testo del GDPR:

- la Guida all'applicazione del Regolamento;
- le FAQ sul Responsabile per la Protezione dei Dati (per quanto di interesse).

Qui di seguito il link di riferimento: <http://www.garanteprivacy.it/regolamentoue/rpd>

A tale ultimo riguardo, tenuto conto delle novità introdotte dalla normativa comunitaria più volte citata (senza pretesa di esaustività), si ritiene di richiamare l'attenzione sui seguenti spunti di rilievo:

- 1) In occasione del primo incontro con il cliente, spesso vengono raccolti i dati anamnestici; in tal caso (trattandosi di dati “sensibili”, peraltro di tipo sanitario), andrà resa un'**informativa** sui diritti di riservatezza con un “linguaggio comprensibile, semplice e chiaro”. È consigliabile acquisire dal cliente un consenso “esplicito”, in forma scritta, per il trattamento dei suoi dati: tale forma scritta, pur non essendo obbligatoria, offre la possibilità al professionista di dimostrare (il concetto di accountability, ovvero di “dimostrabilità” è alla base della nuova normativa) di aver curato tale adempimento;
- 2) Il GDPR introduce il concetto di “non eccedenza” (o “minimizzazione”) nell'utilizzo dei dati, per cui occorre assicurarsi che i dati raccolti siano effettivamente quelli strettamente indispensabili alla cura dei propri pazienti;
- 3) La modalità di conservazione dei dati dovrà garantire non solo la corretta e sicura tenuta degli stessi, ma anche l'esercizio, da parte del paziente, sia del diritto di cancellazione (c.d. “diritto all'oblio”) – che comporta l'obbligo non solo di cancellare i dati in questione, ma anche di informare di ciò altri soggetti che trattino i dati personali cancellati (e di cui, ovviamente si

sia a conoscenza in ragione della propria attività) – sia del diritto di limitazione del trattamento (nei casi di richiesta di rettifica dei dati e di opposizione al trattamento degli stessi);

- 4) Tutti i soggetti, sia interni (colleghi – anche occasionali -, dipendenti, collaboratori, praticanti, tirocinanti ecc.) che esterni (colleghi e soggetti vari esterni: commercialisti, fornitori, personale di pulizia ecc.) devono essere coinvolti nella politica di protezione dei dati e ciò deve risultare, preferibilmente, da atto scritto (sempre per il principio di “dimostrabilità”);
- 5) Occorre definire il tempo di conservazione dei dati personali e ciò, con il GDPR, va esplicitato nell’informativa fornita al paziente (anch’essa, si consiglia, scritta).