

Il 25 maggio 2018 entra in vigore il nuovo Regolamento europeo sulla Protezione dei dati 2016/679.

Con l'entrata in vigore del nuovo RGPD il vecchio D.lgs. 196/2003 non è però da considerarsi abrogato, ma, al contrario, sino a eventuali nuove norme, mantiene la sua forza normativa sul "da farsi" in tema privacy, revisionandosi, integrandosi e aggiornandosi "in chiave GDPR".

Le novità pratiche principali per gli psicologi introdotte dal nuovo Regolamento generale per la protezione dei dati (RGPD) riguardano:

- le modalità di redazione dell'**informativa/consenso** sul trattamento dei dati;
- la predisposizione di un **Registro dei trattamenti dei dati**, ovvero un documento dove si dichiara a priori come si trattano i dati e a quali fini;
- la **gestione** del proprio **archivio professionale** nell'ottica della protezione dei dati trattati;
- **specifico dei passaggi previsti.**

Prima di ogni prestazione professionale, il professionista psicologo sarà obbligato a consegnare l'**informativa/consenso sul trattamento dei dati**, ovvero uno o più documenti in cui vengono chiarite tutte le informazioni, in modo adeguate e comprensibile, riguardanti le modalità di trattamento dei dati personali alla luce del Regolamento europeo 2016/679 (GDPR) e del D. Lgs 196 del 2003 (cd. "Codice Privacy"). L'informativa viene proposta da questo Ordine sul sito istituzionale nella sezione *COME FARE PER – Modulistica – Privacy* in moduli aggiornati in linea con quanto prevede il nuovo GDPR e cumulativo delle altre informazioni/consensi obbligatori.

L'informativa/consenso sul trattamento dei dati redatta alla luce del Regolamento europeo 2016/679 (General Data Protection Regulation) e del D. Lgs 196 del 2003 (cd. "Codice Privacy") è un documento esplicativo che il Titolare del trattamento predispone in forma libera e che deve contenere necessariamente:

- Oggetto del Trattamento
- Finalità del trattamento
- Modalità di trattamento
- Criteri di accessibilità dei dati
- Eventuali comunicazioni/diffusioni dei dati
- Diritti dell'interessato e modalità di esercizio degli stessi
- Dati e contatti di Titolare, responsabile e incaricati

L'informativa va presentata al cliente/paziente a cui vanno forniti tutti i chiarimenti necessari e le spiegazioni richieste assicurandosi di aver adeguatamente informato l'interessato in merito a questioni giuridiche, deontologiche e professionali. A questo punto lo psicologo deve richiedere esplicitamente e in modo chiaro e dimostrabile il consenso al trattamento dei dati; questo deve avvenire necessariamente attraverso l'apposizione della firma in calce all'informativa.

Lo psicologo, nell'ambito del campo di applicazione del GDPR, è inoltre tenuto a trattare e conservare i dati nel proprio archivio secondo indicazioni specifiche e definite in un documento da redigere a cura di ogni professionista, il **Registro dei trattamenti dei dati**.

Il Regolamento, infatti, introduce il principio dell'Accountability: il principio di 'responsabilizzazione' dei Titolari del trattamento che costringe costoro non più (o non soltanto) al rispetto degli obblighi derivanti dal GDPR, ma anche a porsi nelle condizioni di dimostrare di essere in regola, con un giudizio prognostico basato su di un processo di valutazione dei rischi, coerente allo scopo e composto da adeguate misure e procedure interne preventive.

Questo documento, da conservare di norma ove si esercita la propria attività professionale, rappresenta il "manuale di istruzioni" in cui ogni professionista è tenuto semplicemente ad esplicitare chiaramente da chi e come saranno trattati i dati, dall'informativa all'archiviazione. Esso rappresenta anche il riferimento, in caso di controllo da parte dell'autorità giudiziaria, al quale nella pratica operativa ognuno dovrà necessariamente attenersi.

Per quanto riguarda la **gestione dell'archivio professionale**, questo dovrà essere sempre suddiviso fra dati personali del cliente/paziente, soggetti a tutto quanto previsto dal GDPR e sempre dovuti in caso di richiesta del cliente/paziente, forniti dall'interessato direttamente o osservati e raccolti nella loro forma di dati grezzi generati da un "contatore intelligente" o altri elementi oggettivi di raccolta (ad es. scritti dell'interessato, fotografie, prodotti audio video, i punteggi grezzi di un test, risposte a questionari, i disegni, dati oggettivi di qualsiasi tipo) e dati professionali dello psicologo, legati alla sua attività, prodotti dal professionista, sempre soggetti a procedure di trattamento secondo il GDPR ma non necessariamente dovuti al cliente/paziente (appunti, relazioni, valutazioni, interpretazioni ecc..).

Alcuni aspetti tecnico-normativi e alcune novità del GDPR

Il Nuovo Regolamento, nei suoi principi fondanti, si pone nell'alveo della direttiva 95/46/CE e del Codice Privacy, infatti in base all'art. 5 del GDPR i dati personali sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato ('liceità, correttezza e trasparenza');
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ('limitazione della finalità');
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ('minimizzazione dei dati');
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ('esattezza');
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente GDPR a tutela dei diritti e delle libertà dell'Interessato ('limitazione della conservazione');
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ('integrità e riservatezza');

Con il GDPR vengono, poi, rafforzati i diritti degli utenti (interessati al trattamento) e quindi:

- **Diritto di accesso (art. 15):** l'Interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e a determinate informazioni specificamente indicate (finalità del trattamento, destinatari o categorie di destinatari cui i dati sono o saranno comunicati, periodo di conservazione dei dati, diritti dell'Interessato, esistenza di un processo decisionale automatizzato, compresa la profilazione, ecc.)
- **Diritto di rettifica (art. 16):** l'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
- **Diritto alla cancellazione ('diritto all'oblio', art. 17):** in determinati casi l'Interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo.

- Diritto di limitazione del trattamento (art. 18): in determinati casi l'Interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento (alla sola operazione di conservazione dei dati personali);
- Diritto alla portabilità dei dati (art. 20): qualora il trattamento si basi su consenso o su contratto e sia effettuato con mezzi automatizzati, l'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e ha il diritto di trasmettere tali dati ad altro Titolare senza impedimenti da parte del primo.
- Diritto di opposizione (art. 21): l'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione.
- Informativa: l'Interessato ha diritto ad essere informato dell'esistenza del trattamento e delle sue finalità e delle ulteriori circostanze necessarie alla sua tutela; l'Interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa.

Inoltre in base all'art. 25, è necessario che il Titolare si organizzi secondo i principi della Privacy by default e Privacy by design. Privacy by design, significa protezione dei dati fin dalla progettazione/ideazione di un qualsiasi prodotto, servizio, applicativo, software o sistema informatico che tratti dati personali. Privacy by default, significa tutela della vita privata dei cittadini grazie a un'impostazione predefinita dell'organizzazione dello Studio atta a garantirla.

Ulteriori novità sono poi le seguenti:

- Data Breach (art. 32 ss. GDPR): il data breach è un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezza in maniera involontaria o volontaria (es. perdita accidentale, furto, infedeltà aziendale, accesso abusivo).
- La violazione dei dati personali deve essere notificata al Garante entro 72 ore e comunicata all'Interessato dal Titolare del trattamento.

Lo psicologo libero professionista, dato l'esiguo numero di dati trattati e l'attività di norma svolta in modo individuale, è sempre Titolare del trattamento dei dati e non è tenuto, come invece sono tenute altre realtà professionali, alla nomina di un Responsabile Protezione Dati.