

Gli psicologi e la privacy, cosa cambia?

Dal 25 maggio 2018 cambia il quadro normativo in materia di protezione dei dati personali, fortemente modificato dall'entrata in vigore del **Regolamento europeo 2016/679 (General Data Protection Regulation – di seguito “GDPR” o “Regolamento”)**.

Fino ad oggi la tutela dei dati personali era affidata alla direttiva 95/46/CE, recepita da ciascuno Stato membro dell'Unione Europea con proprie norme locali. In Italia la direttiva fu recepita con il ben noto **D.Lgs 196 del 2003 (cd. “Codice Privacy”)** che ad oggi ha rappresentato a livello italiano il riferimento centrale, culturale e burocratico, per il trattamento di tutti i dati personali.

Con l'entrata in vigore del GDPR 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”.

Questo nuovo Regolamento ci aiuterà perché, pur non comportando un cambiamento radicale nel modo in cui abbiamo trattato la materia finora nel nostro esercizio professionale, è ben strutturato, chiaro e più rigoroso delle precedenti normative.

Nello specifico della professione di psicologo esso armonizza le norme di trattamento dei dati con i principi e le modalità degli altri adempimenti basati su informative, consensi espliciti, opposizione e archiviazione sistematica e strutturata.

Le novità pratiche principali riguarderanno:

- la predisposizione di un documento (**Valutazione d'Impatto**) in cui lo psicologo dichiara a priori come tratterà i dati;
- le modalità di redazione dell'**Informativa** e l'importanza dell'effettività nella modalità di informazione/consenso;
- La gestione dell'**Archivio professionale**;
- Le sanzioni molto più severe;
-

Il nuovo Regolamento Europeo rappresenta quindi l'opportunità per responsabilizzarsi, riunificare e comprendere meglio alcuni degli obblighi

contrattuali, legali e deontologici, cui ogni psicologo dovrebbe adempiere nel proprio esercizio professionale.

Vi forniamo con questa nota alcune prime linee guida generali, tuttavia, l'invito del Consiglio Nazionale a tutti gli Ordini territoriali, a tutti i colleghi e a tutte le realtà del mondo psicologico, è chiaramente quello di approfondire ulteriormente, ovunque possibile, con momenti informativi e formativi, individuali o collettivi tutte le attualissime implicazioni nello specifico del nuovo **Regolamento europeo 2016/679**.

Sarà altresì presto disponibile anche una guida più estesa, realizzata dalla Commissione Giuridico Istituzionale del CNOP, in merito a tutte le altre norme che impattano ad oggi sulla nostra professione: IL DECALOGO NORMATIVO DELLO PSICOLOGO - Gli obblighi formali minimi per esercitare la professione. In allegato a tale pubblicazione sarà possibile reperire anche un modello esemplificativo generico, il **modello psy2018**, che unifica e semplifica tutto quanto richiesto in materia di privacy, consenso informato, preventivo, sistema tessera sanitaria.

Privacy e segreto professionale dello psicologo: informative, opposizione/consenso, firme

Lo psicologo è un professionista che interviene sempre, per definizione, sulla **salute** di individui gruppi e comunità e per tale motivo ogni psicologo nel proprio lavoro entra necessariamente in contatto con **dati comuni (o identificativi)** e con **dati sensibili**, che assieme costituiscono l'insieme dei cosiddetti **dati personali** di un interessato.

Il lavoro dello psicologo è già profondamente caratterizzato dai principi di tutela di tutto quanto appreso in ragione del rapporto professionale in virtù di quanto previsto dal **Codice Deontologico degli Psicologi Italiani**. Il corretto esercizio della professione è quindi già di base coerente con un corretto trattamento dei dati. Moltissimi articoli del Codice, infatti, rimandano o si integrano perfettamente con i principi del GDPR: art. 2 (corretto esercizio della professione), art. 3 (responsabilità sociale), art. 4 (diritto alla riservatezza), art. 9 (ricerca scientifica), art. 11 (segreto professionale), art. 12 (testimonianza e deroga al segreto), art. 13 (obbligo di referto e obbligo di denuncia), art. 14 (gruppi), art. 15 (supervisione, condivisione, collaborazione interprofessionale), art. 16 (anonimato nelle comunicazioni

scientifiche), art. 17 (custodia dei dati), art. 24 (consenso informato), art. 31 (consenso informato minori).

In merito alla contrattualizzazione dello psicologo con i propri clienti/pazienti sono recentemente subentrate anche altre nuove e differenti norme come **l'obbligo di preventivo** e la **trasmissione telematica delle spese sanitarie al "sistema tessera sanitaria"**.

Tutto ciò premesso,

PRIMA di ogni prestazione professionale, **il professionista psicologo sarà quindi sempre obbligato** a:

- consegnare l'**informativa (o delle Informative)**, 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 / privacy** alla luce del Regolamento europeo 2016/679 (*General Data Protection Regulation*) e del D.Lgs 196 del 2003 (cd. "Codice Privacy"); le prestazioni, le finalità e le modalità delle stesse, nonché circa il grado e i limiti giuridici della riservatezza alla luce del **consenso informato** secondo il Codice Deontologico; quanto richiesto **dall'obbligo di preventivo** ai sensi della L. n.124/2017; e, in caso di prestazione sanitaria, i riferimenti e chiarimenti in merito alla **trasmissione telematica delle spese sanitarie** all'Agenzia delle Entrate.

N.B. L'**informativa** 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, 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

Dopo la presentazione dell'informativa/e, dopo aver fornito tutti i chiarimenti necessari e le spiegazioni richieste, assicuratosi di aver, appunto, adeguatamente informato l'interessato in merito a questioni giuridiche, deontologiche e professionali, lo psicologo deve richiedere esplicitamente e in modo chiaro e dimostrabile o l'opposizione o le **firme**:

- ✓ al **consenso informato** (art.24 o art.31 C.D.) e **l'accettazione del preventivo** (L. n.124/2017) → firma 1
- ✓ al **consenso al trattamento dei dati personali** (D.Lgs 196 del 2003 / GDPR 679/16) → firma 2

In assenza di questi passaggi preliminari non è possibile effettuare nessuna prestazione professionale.

(in caso di prestazioni sanitarie è altresì necessario)

- ✓ **alla trasmissione telematica delle spese sanitarie** (ex art.24 o art.31 C.D. → firma 3

DOPO la prestazione professionale, lo psicologo, nell'ambito del campo di applicazione del GDPR, è 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, la **valutazione d'impatto**.

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.

Tale 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 altresì il riferimento, in caso

di controllo da parte dell'autorità giudiziaria, cui nella pratica operativa ognuno dovrà necessariamente attenersi.

L'archivio dovrà inoltre 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 Garante¹ entro 72 ore e comunicata all'Interessato dal Titolare del trattamento.

- **DPO (Data Protection Officer)**, ovvero un Responsabile della Protezione dei Dati (RPD).

N.B. 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 ma non è strettamente tenuto alla nomina di un RPD.

¹ <http://www.garanteprivacy.it>