STUDIO LEGALE DURANO
Via Palestro, 5 - 72100 Brindisi (BR)
T. 0831 529698 - F. 0831 560971
www.studiolegaledurano.it

Il Nuovo Regolamento Privacy n. 679/2016 (c.d. GDPR) per gli studi legali

Ormai da alcuni mesi (25 maggio 2018) è entrato in vigore il Regolamento UE n. 679/2016 in materia di protezione dei dati personali delle persone fisiche (e non anche delle persone giuridiche, innovando sul punto l'ambito di applicazione del Codice Privacy italiano di cui D.Lgs. n. 196/2003).

Sul versante interno, è entrato in vigore il 19 settembre u.s. il decreto legislativo di adeguamento al GDPR n. 101/2018.

Tra le disposizioni del D.Lgs. n. 101/2018, l'art 22, punto 13, ha previsto che "*Per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie*."

La nuova disciplina, dunque, impone – seppur con il temperamento di cui si è detto – il necessario adeguamento anche da parte degli studi legali, per tutelare i dati trattati relativi agli interessati (clienti, fornitori, dipendenti, controparti) ed evitare che la divulgazione, anche accidentale, possa ledere i diritti degli stessi.

Invero, si tratta di precauzioni che dovrebbero essere già comprese - e in ogni caso si coniugano perfettamente con - il rispetto degli obblighi deontologici della professione forense, a partire dall'obbligo di garantire il segreto professionale e di tutela del rapporto di confidenzialità che si crea tra avvocato e cliente.

Le nuove disposizioni in materia di privacy, tuttavia, impongono oneri che, se anche non eccessivamente gravosi per gli avvocati i quali erano già tenuti ad una serie di adempimenti obbligatori di natura informativa nei confronti dei loro clienti, devono essere assolti, pena le passibili irrogazioni di salate sanzioni da parte del Garante.

Di seguito, in pillole, il GDPR per gli avvocati:

- **RESPONSABILITÀ**

Uno dei principi fondamentali del Regolamento è quello dell'*accountability*, ovvero della responsabilità del Titolare del trattamento: l'inosservanza del richiamato principio comporta l'applicazione di ammonimenti, avvertimenti, limitazioni e ordini, sanzioni amministrative da parte del Garante per la protezione dei dati personali.

Nell'ipotesi degli studi legali, il prinicpio di *accountability* importa che il legale deve essere garante della conformità al Regolamento dei trattamenti da esso stesso posti in essere dei dati personali di cui egli entra in possesso.

❖ **INFORMATIVA**

L'articolo 13 del Regolamento impone che i clienti vengano informati su:

- identità e dettagli di contatto dell'avvocato o dell'associazione o società professionale;
- le finalità del trattamento dei dati;
- la base giuridica del trattamento;
- i destinatari dei dati (ad esempio gli uffici giudiziari);
- i flussi transfrontalieri;
- la durata della conservazione;
- i diritti che gli interessati possono esercitare;
- le condizioni per l'esercizio dei diritti degli interessati;
- il diritto di revocare il consenso;
- il diritto di presentare un reclamo all'autorità di controllo;
- le informazioni sulla natura del trattamento.

L'informativa contenente tutte queste informazioni deve essere resa in modo chiaro e comprensibile, può essere resa in formato cartaceo o elettronico (per esempio, via e- mail), può essere fornita anche nel corpo dell'accordo contrattuale o inserita sul sito WEB (in questo caso è onere dell'avvocato dimostrare che essa è stata letta e compresa, per esempio, inserendo nel testo della procura la presa visione e la dichiarazione di comprensione dell'informativa).

❖ **CONSENSO E CONDIZIONI DI LICEITA' DEL TRATTAMENTO**

Il consenso è definito dall'art. 4, par. 1 n. 11, del GDPR come "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

L'art. 6, par. 1, del GDPR indica 5 condizioni di liceità del trattamento alternative tra loro nel senso che almeno una deve ricorrere affinché il trattamento possa essere considerato lecito. Delle condizioni indicate, si evidenziano le seguenti:

- l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario **all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Quantunque non sia richiesto un consenso scritto, e sebbene l'attività professionale possa rientrare nell'ipotesi 2, è preferibile precostituirsi la prova di

avere ottenuto il consenso (art. 7, par. 1, del GDPR): l'avvocato, quindi, dovrà sottoporre al cliente per la firma una dichiarazione di consenso in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive.

È facoltà dell'interessato revocare il proprio consenso in qualsiasi momento (art. 7, par. 2, del GDPR), ma "*la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca*".

❖ REGISTRO

All'articolo 30, il Regolamento prevede l'obbligo di **tenuta di un registro delle attività di trattamento**, ma si tratta di un onere non obbligatorio per i titolari di trattamento dei dati in strutture con meno di 250 dipendenti, a meno che il trattamento non includa un rischio per i diritti e le libertà degli interessati oppure se si riferisca a dati sensibili o relativi a condanne o reati.

In sostanza, **questo adempimento ricade sui grandi studi legali e sugli avvocati che si occupano di diritto penale, famiglia e minori, previdenza sociale, responsabilità medica e in generale di vertenze in materia di risarcimento danni da lesioni personali**.

Il registro individua:

- il titolare del trattamento;
- le categorie dei dati trattati;
- le finalità;
- le persone coinvolte nel trattamento;
- le categorie dei destinatari a cui i dati personali sono o saranno comunicati, compresi i destinatari in paesi terzi;
- il termine ultimo previsto per la cancellazione dei dati;
- la descrizione delle misure di sicurezza tecniche e organizzative dello studio per garantire la riservatezza dei dati.

  Anche in questo caso, uno schema del registro dei trattamenti è disponibile e scaricabile sul sito del CNF.

❖ DATA BREACH

Per *data breach* si intende la **violazione dei dati personali che presenti un rischio per i diritti e per le libertà delle persone fisiche**.

Ancorché si tratti di un'ipotesi improbabile nel caso dei dati trattati da un avvocato, qualora un legale ritenga che una violazione dei dati personali in suo possesso si sia verificata deve comunicare tale evento al Garante e al diretto interessato entro e non oltre 72 ore dalla presa di coscienza di una violazione della sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, l'alterazione, la divulgazione o l'accesso di persone non autorizzate ai dati personali da lui conservati.

❖ PORTABILITÀ DEI DATI

Il diritto alla portabilità dei dati attribuisce agli interessati la facoltà di esigere dal titolare del trattamento la trasmissione dei loro dati ad un altro titolare, senza che il primo si possa opporre.

L'art. 20 del GDPR attribuisce all'interessato 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 ed ha il diritto di trasmettere tali dati a un altro titolare del trattamento, senza impedimenti da parte del titolare del trattamento cui li ha forniti, qualora:

- il trattamento si basi sul consenso o su un contratto
- il trattamento sia effettuato con mezzi automatizzati.

Ciò significa che **l'avvocato che tratti i dati dei clienti con mezzi automatizzati** (per esempio, adottando un gestionale informatico o anche solo tenendo uno schedario sotto forma di foglio di calcolo) **è tenuto a comunicare i dati del suo cliente al collega se il cliente ha espresso il suo consenso al trattamento dei suoi dati personali o il trattamento è necessario per l'esecuzione di un contratto di cui il cliente è parte**.

Pertanto, se il suo cliente richiede la trasmissione dei suoi dati ad un collega, l'avvocato dovrà trasferirli in formato strutturato comunemente usato e leggibile da una macchina.

Il diritto alla portabilità si applica solo se il trattamento è effettuato con l'aiuto di procedure automatizzate, e pertanto **non sarebbe esteso ai fascicoli cartacei**, che sembrano dunque esclusi dal diritto alla portabilità. Deve però essere ricordato che, secondo l'art. 2235 c.c., l'avvocato non ha diritto a trattenere i dati se non il tempo necessario alla tutela dei propri diritti.

Peraltro, il diritto alla portabilità non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

❖ CONSERVAZIONE DEI DATI

L'avvocato titolare del trattamento deve definire una politica di durata e di conservazione dei dati nel suo ufficio.

I dati personali possono essere conservati solo per il tempo necessario per il completamento dell'obiettivo perseguito durante la loro raccolta.

In generale, i dati dei clienti possono essere tenuti per la durata del mandato professionale tra l'avvocato e il suo cliente.

Possono ovviamente essere conservati anche dopo la cessazione del rapporto professionale, al fine di tutelare i diritti dell'avvocato nei confronti del cliente, sia quanto al **diritto a conseguire i compensi**, sia per **resistere ad eventuali azioni di responsabilità**: per tale ragione, si ritiene che la conservazione dei dati possa prolungarsi per tutto il tempo di prescrizione ordinaria, prima della loro cancellazione definitiva.

È, inoltre, importante ricordare che i dati acquisiti in sede di identificazione e adeguata verificata ai sensi del decreto legislativo n. 231 del 2007 in materia di antiriciclaggio devono essere conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale (art. 31, comma 3, d. lgs. 231 del 2007).

❖ DIRITTO DI ACCESSO AI DATI

Il GDPR apporta le rilevanti modifiche anche sul diritto di accesso ai dati da parte dell'interessato.

Qualsiasi persona fisica che giustifichi la sua identità ha diritto di interrogare il titolare:

- per sapere se sta trattando i suoi dati;
- per ottenere la comunicazione dei dati in forma comprensibile e tutte le informazioni disponibili per quanto attiene l'origine del trattamento;
- per ottenere informazioni sulla finalità del trattamento i dati raccolti e i destinatari.
  Il tempo di risposta è stato fissato in un mese dal ricevimento della richiesta (articolo 12.3).

Viene tuttavia offerta l'opportunità di prorogare questo termine di due mesi, "*data la complessità e il numero di applicazioni*", a condizione che l'interessato riceva comunque un'informazione al riguardo entro un mese dal ricevimento della richiesta (articolo 12.3).

Il regolamento prevede un principio di gratuità copie fornite come parte di una richiesta di accesso (Articolo 12.5) tranne nei casi di domande manifestamente infondate o eccessive per le quali il responsabile del trattamento può richiedere il pagamento di "*costi ragionevoli*" che tengono conto dei costi amministrativi sostenuti per la fornitura delle informazioni. La medesima regola si applica quando viene richiesta una copia aggiuntiva dei dati.

Il regolamento prevede che se la persona inoltra una domanda per via elettronica, l'informazione richiesta è comunicata in forma elettronica di uso comune, a meno che l'interessato non richieda diversamente (art. 12,3).

Prevede inoltre che il responsabile del trattamento assista il titolare nell'adempimento dei suoi obblighi riguardo al diritto di accesso (articolo 28).

❖ AVVOCATO DOMICILIATARIO

L'**avvocato mero domiciliatario**, poiché tratta dati personali per conto del *dominus* mandatario (titolare del trattamento) riveste la qualifica di **Responsabile del trattamento ai sensi dell'art. 28 GDPR**.

I responsabili del trattamento sono soggetti ad oneri ed obblighi del tutto similari a quelli previsti per i titolari, devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

I domiciliatari non potranno ricorrere ad altri responsabili o sub-responsabili senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento ed in ogni caso, dovranno informare immediatamente del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare l'opportunità di opporsi a tali modifiche.

❖ DATI TRATTATI IN UNO STUDIO LEGALE

In uno studio legale vengono trattati, generalmente le seguenti categorie di dati:

- relativi al personale dipendente ed ai collaboratori;
- relativi ai clienti;
- raccolti attraverso il sito internet.

Per tutte le categorie valgono le medesime regole e, quindi, è necessario procedere agli opportuni adeguamenti.

❖ ADOZIONE DI BUONE REGOLE PER LA SICUREZZA DEI DATI

Come già si è detto, è essenziale garantire la sicurezza e la riservatezza dei dati trattati dagli studi legali garantendo un livello di sicurezza adeguato al rischio di trattamento.

L'avvocato è soggetto al segreto professionale.

Questo obbligo rafforza la necessità di misure di sicurezza negli studi legali poiché in caso di violazione dei dati personali dei clienti, è il segreto professionale che viene violato.

La sfida della sicurezza è dunque di importanza vitale per l'avvocato e, per nulla, scontata

È necessario mettere in atto misure di sicurezza fisica nello studio, come ad esempio:

- limitare l'accesso allo studio;
- Non archiviare fascicoli o documenti contenenti dati personali in locali dello studio accessibili a tutti;
- Dotare i computer di una password minima di 8 caratteri contenenti maiuscole, lettere minuscole, numeri e caratteri speciale;
- determinare persone che hanno il diritto di accedere ai dati personali;
- rimuovere le autorizzazioni di accesso obsolete;
- scrivere un regolamento di utilizzo del computer e inserirlo nel regolamento interno nell'ipotesi che sia stato adottato
- fornire mezzi di crittografia per computer portatili e dispositivi di archiviazione rimovibili (chiavette USB, CD, DVD …)
- evitare di memorizzare dati personali sensibili dei clienti.
- eseguire il backup e pianificare la business continuità
- implementare i backup regolarmente, conservare i supporti di backup in un luogo sicuro

❖ SANZIONI

Titolari e responsabili del trattamento possono essere soggetti a sanzioni amministrative significative per il mancato rispetto delle disposizioni del GDPR.

L'autorità Garante per la protezione dei Dati personali, può, in particolare:

- rivolgere avvertimenti;
- ammonire l'avvocato, l'associazione o la società professionale;
- limitare temporaneamente o permanentemente un trattamento;
- sospendere i flussi di dati;
- ordinare di soddisfare richieste per l'esercizio dei diritti delle persone;
- ordinare la rettifica, limitazione o cancellazione dei dati
- ritirare la certificazione di conformità concessa all'avvocato, allo studio, all'associazione o alla società professionale, ovvero ordinarne il ritiro all'autorità di certificazione;
- comminare una sanzione amministrativa fino ad importi compresi tra i 10 ed i 20 milioni di euro, ovvero, in caso di grandi studi internazionali di importo compreso tra il 2% ed il 4% del fatturato mondiale.