

Adempimenti

Privacy e studi legali: il nuovo Regolamento europeo

Monica Lambrou - Avvocato

L'entrata in vigore del Regolamento Ue sulla privacy 2016/679, produce significativi effetti, tra gli altri, anche sugli aspetti inerenti la gestione degli studi legali da parte di coloro i quali svolgono la professione di avvocato. Trattasi, in particolare, dell'entrata in vigore di nuovi e inediti adempimenti, concernenti, in primo luogo, l'acquisizione del consenso da parte degli interessati, nonché le modalità di trattamento e di relativa conservazione dei dati.

Occorre preliminarmente rilevare come, con l'intervento legislativo in oggetto, il legislatore europeo abbia inteso uniformare la disciplina vigente nei Paesi Membri in merito al trattamento dei dati personali, offrendo alla totalità dei cittadini dell'Unione europea un meccanismo di tutela particolarmente garantista e, soprattutto, omogeneo in tutto il territorio comune. I legislatori nazionali saranno, di conseguenza, chiamati a dotarsi di discipline interne, sia al fine di attuare talune delle disposizioni e delle prescrizioni previste dal Regolamento in oggetto, sia al fine di dotarsi di propri meccanismi di garanzia e di tutela. Anche per quanto riguarda il Legislatore italiano, in particolare, il procedimento di emanazione del Decreto legislativo consente di adeguare la disciplina nazionale a quella europea. Particolare attenzione dovrà, in questo senso, essere rivolta alle modalità di raccordo tra il Regolamento Ue 2016/679 e il Decreto legislativo 30 giugno 2003, n. 196 (c.d. Codice della privacy).

Ad ogni modo, in un quadro generale di riordino, nonché di previsione di nuove e ingenti sanzioni in caso di violazioni alle prescrizioni normative, l'avvocato sarà chiamato a prestare particolare attenzione nello svolgimento della propria attività professionale, nonché a sostenere maggiori oneri economici per un corretto trattamento dei dati personali dei propri clienti e collaboratori, risultando, talvolta, necessario, a tal fine, l'ausi-

lio e la collaborazione di figure terze ed esterne allo studio. Per la natura dell'attività professionale svolta, infatti, l'avvocato si ritrova costantemente - e quotidianamente - a trattare dati personali dei suoi clienti a vario titolo. Ai fini del corretto esercizio delle proprie incombenze, il professionista è titolare del trattamento sia in fase giudiziale, sia in fase stragiudiziale, ma anche nell'ambito di un mero colloquio conoscitivo e di richiesta di consulenza. Nell'ambito degli studi legali, poi, detto trattamento si rende necessario altresì in capo ai collaboratori del titolare dello studio, tra questi i praticanti avvocati, che (invero, già sulla base di quanto disposto dal "vecchio" Codice della privacy e dai chiarimenti successivi del Garante della privacy, Doc-Web 1007280 del 3 giugno 2004) devono, ai fini della liceità dell'attività dagli stessi svolta, essere espressamente nominati quali incaricati del trattamento. In tal senso, occorre specificare che il nuovo Regolamento, a dispetto di quanto disciplinato dal Codice della privacy del 2003, non prevede espressamente la figura dell'"incaricato del trattamento", ma non v'è dubbio nel ritenere che analoghi adempimenti e obblighi sorgano nei confronti dei collaboratori di studio in qualità di "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*" (si veda, in questo senso, articolo 4, n. 10, Regolamento Ue 2016/679). Peraltro, lo stesso Garante per la protezione dei dati personali, con la propria "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali", nel chiarire le principali problematiche a cui imprese (nonché professionisti) dovranno prestare particolare attenzione, ha provveduto a confermare, a livello interpretativo, la perfetta coincidenza tra l'"incaricato", di cui al D.Lgs. n. 196/2003, e la "*persona autorizzata*" di cui al Regolamento Ue 2016/679, sia in merito

Approfondimenti

alle relative caratteristiche soggettive che all'ambito della responsabilità.

Quanto sopra vale, in ogni caso, non solo ove il trattamento riguardi i generici dati identificativi dei clienti e degli altri soggetti coinvolti in un caso, ma anche e soprattutto per i c.d. "dati sensibili" che lo stesso Regolamento individua in tutte le informazioni idonee a rivelare "*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o, l'appartenenza sindacale*" (così come definiti dal Regolamento Ue, 2016/679 all'articolo 9, comma 1). Sotto tale profilo, basti al momento rilevare che il professionista, ai fini della liceità del trattamento dei dati di cui sopra, dovrà ottenere dall'interessato un consenso esplicito e specificatamente riferito a dette informazioni "*per una o più finalità specifiche*".

Ciò premesso, giova analizzare nel dettaglio le principali novità che riguardano direttamente l'avvocato e il relativo studio nello svolgimento della professione forense e nel rapporto con le persone fisiche (per costante giurisprudenza, invero, la tutela dei dati personali non può in alcun modo intendersi estesa alle persone giuridiche).

I principi di accountability e di privacy by design

Al pari di aziende ed enti pubblici, gli studi legali saranno chiamati al rispetto e all'applicazione concreta dei principi fondamentali posti alla base del Regolamento e della concezione di tutela della privacy dallo stesso promossa. Trattasi, in particolar modo, del principio di *accountability* e di *privacy by design*.

Ebbene, "responsabilizzazione" è il precetto cui far discendere qualsivoglia azione a tutela dei dati personali. L'avvocato - seppur in presenza di taluni rilevanti vincoli legislativi - può dotarsi di una propria autonoma organizzazione, nonché scegliere le modalità cui dar luogo al trattamento dei dati, purché tale opzione possa rivelarsi, in una valutazione successiva, adeguatamente efficace. Lo stesso dovrà, infatti, dimostrare l'efficacia delle misure adottate, la cui aderenza al dato legislativo andrà valutata sulla base del contesto in cui opera. Appare del tutto evidente come, in considerazione della richiamata rilevanza dei dati personali trattati all'interno di uno studio legale,

tali misure debbano caratterizzarsi per incisività e, talvolta, radicalità.

Va, in primo luogo, garantita la trasparenza della propria attività e della gestione dei dati che offra al cliente la possibilità di accedere in ogni momento alle proprie informazioni e di avvalersi, con riscontri tempestivi, dei diritti che, a vario titolo, il Regolamento prescrive. Si pensi, in questo senso, oltre al citato diritto d'accesso (articolo 15, Regolamento Ue, 2016/679), al diritto di rettifica (articolo 16), al diritto di cancellazione o "diritto all'oblio" (articolo 17), al diritto di limitazione del trattamento (articolo 18) e, in particolare, al diritto di revocare il proprio consenso precedentemente espresso. In applicazione di tali principi, il riscontro dell'avvocato in merito alle richieste non può avere luogo oltre i trenta giorni (decorrenti dal giorno in cui è effettivamente avvenuta la richiesta dell'interessato), fatto salvo il diritto del cliente di adire l'Autorità di controllo (articolo 77), costituita, nell'ordinamento italiano, dal Garante per la protezione dei dati personali.

Occorre che gli avvocati, per di più, si dotino di effettive misure di sicurezza, da attuarsi in seguito ad una preventiva valutazione dei rischi insiti nell'attività professionale di ciascuno. In altri termini, allo stesso modo delle imprese, il professionista è chiamato ad abbandonare la logica di mero rispetto delle prescrizioni legislative e dei limiti dalle stesse imposte, in favore di un approccio sostanziale, anche adeguando la propria *policy* interna sulla base dei rischi di volta in volta riscontrati.

Particolare attenzione, poi, dovrà prestarsi con riferimento agli strumenti tecnologici ed informatici utilizzati all'interno dello studio legale. In forza del principio di *privacy by design*, la tutela della riservatezza dei clienti (ciò vale anche per i dati riferibili ai collaboratori) e la relativa efficacia andrà valutata anche in relazione a detti strumenti. Oltre alle semplici cautele che impongono, a titolo meramente esemplificativo, di non lasciare aperti e incustoditi *files* contenenti i dati personali, parrebbe opportuna l'adozione di interventi minimi tra cui:

- in caso di utilizzo di *software* gestionali per studi legali, molto diffusi nella pratica, verificare la serietà della società terza nella predisposizione del programma e della relativa modalità di raccolta e conservazione dei dati, nonché nell'ido-

neità dello stesso a garantire sicurezza e anonimizzazione;

- garantire l'accesso ai dati ai collaboratori di studio con l'ausilio di *password*, o altri metodi di protezione, che consentano la visualizzazione esclusiva delle informazioni per le quali il collaboratore sia stato preventivamente autorizzato e per le mansioni cui sia stato effettivamente adibito;
- aggiornare costantemente i propri programmi *firewall* e antivirus, per evitare l'illecito accesso di terzi e, ove ciò sia concretamente possibile, dotarsi dei c.d. "software antintrusione";
- effettuazione periodica di un *back up* dei dati contenuti.

Trattamento cartaceo dei dati

Da una lettura attenta del testo del Regolamento non parrebbero emergere particolari indicazioni ulteriori (rispetto a quanto già disposto dal Codice della privacy) in merito alle modalità di conservazione cartacea dei fascicoli contenenti i dati personali dei clienti. Possono, con ciò, dirsi ancora valide le indicazioni offerte dal Consiglio nazionale forense che, con il proprio "Vademecum per gli studi legali concernente gli adempimenti richiesti dal Codice della privacy" era intervenuto a chiarire la necessità di talune pratiche cautelative.

In particolare, occorre sinteticamente rilevare come, sulla base di tale documento, sia possibile apporre sul fascicolo "un numero identificativo nonché il nome del cliente e delle parti", ma debba ritenersi, in ogni caso, consigliabile "che i nomi siano evidenziati solo all'interno del fascicolo". Il fascicolo deve, comunque, essere conservato in luoghi riservati che - senza la necessità di una protezione sotto-chiave - non vedano l'accesso diretto né di clienti né di terzi senza opportuna autorizzazione.

Consenso e informativa

La regola generale già prevista dal Codice della privacy, in merito alla necessità di ottenere preventivamente il consenso dell'interessato ai fini del trattamento, continua ad operare anche con il Regolamento Ue. Invero, a norma dell'articolo 6 comma 1, detto trattamento è da intendersi lecito se, appunto, "l'interessato ha espresso il consen-

so al trattamento dei propri dati personali per una o più finalità specifiche".

Orbene, in questo senso, si pone un problema interpretativo del tutto rilevante ai fini dell'esercizio della professione di avvocato. Occorrerà, infatti, valutare se, in virtù della maggior coerenza e pregnanza della normativa europea, continueranno ad essere attuali i principi espressi dal Garante per la protezione dei dati personali in merito al trattamento dei dati sensibili.

Con l'Autorizzazione n. 4 del 15 dicembre 2016, nonché con le nn. 5, 6 e 7, invero, l'Autorità di controllo era giunta a concedere agli avvocati, nonché ad altri liberi professionisti iscritti negli appositi albi, l'autorizzazione al trattamento dei dati sensibili dei clienti senza consenso specifico allorché proporzionato alla propria attività di rappresentanza e assistenza, con possibilità di comunicazione a terzi "nei limiti strettamente pertinenti all'espletamento dell'incarico conferito". In tal senso, bisognerà attendere nuove pronunce del Garante e la relativa interpretazione, prestando, in particolare, attenzione alla compatibilità delle predette autorizzazioni con la disciplina che il Regolamento Ue appronta alle finalità del trattamento (si leggano, in questo senso, i principi di cui all'art. 5, Regolamento Ue 2016/679).

Ad ogni modo, analogamente a quanto disposto dall'art. 13, Codice della privacy, sulla base dell'art. 13, Regolamento Ue, 2016/679, l'avvocato sarà chiamato a predisporre un'ideale informativa in favore del cliente al momento di acquisizione dei relativi dati personali.

Cosa cambia, in questo senso, con riferimento al contenuto dell'informativa e alla sua redazione?

- L'informativa dev'essere resa per iscritto o con altri mezzi, in forma concisa, trasparente, intelligibile, facilmente accessibile e con un linguaggio semplice e chiaro. La disciplina di cui al Codice della privacy non poneva particolari limiti alla trasmissione delle informazioni in forma orale; il Regolamento, ove prevede che, se richiesto dall'interessato, "l'informativa è da rendere oralmente" parrebbe privare del tutto di tale opzione il titolare del trattamento;

- occorre fornire idonee informazioni circa la base giuridica del trattamento (non richieste espressamente dal Codice del 2003), ossia se lo stesso derivi da una norma, da un contratto, ovvero da una richiesta dell'interessato;

Approfondimenti

- occorre rendere edotto l'interessato della facoltà o meno di rifiutare di fornire i propri dati, specificandone, altresì, le conseguenze;
- occorre indicare il periodo di conservazione dei dati, ovvero i criteri utilizzati per determinarlo;
- occorre implementare l'elencazione e il riepilogo dei diritti di cui all'articolo 7 del Codice della privacy, con i nuovi diritti previsti dal Regolamento Ue, esplicitando, altresì, la possibilità per il cliente di proporre reclamo al Garante ai sensi dell'articolo 77;
- occorre indicare il nominativo del Responsabile della protezione dei dati (D.P.O.), qualora questi sia stato nominato.

Va detto che gli adempimenti di cui sopra risulteranno necessari altresì con riferimento ai dati già raccolti al momento dell'entrata in vigore del Regolamento Ue e si ritiene, con ciò, del tutto opportuno rivedere le informative e i consensi già prestati dai clienti.

Il responsabile della protezione dei dati

L'introduzione del c.d. D.P.O. (Data Protection Officer) rappresenta una delle novità di maggior rilievo nell'ambito della nuova normativa. Questi rivestirà il ruolo di vero e proprio sovrintendente in materia di privacy all'interno dei contesti aziendali, con svariati compiti che possono così riassumersi:

- consulenza al titolare del trattamento con riferimento alla normativa europea e nazionale sulla privacy;
- formare e sensibilizzare il personale che si ritrovi, nello svolgimento delle proprie mansioni, a trattare dati personali;
- cooperare con il Garante della privacy, fungendo da punto di contatto tra lo stesso e il contesto in cui opera;
- sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati richiesta alle imprese e fornire parere in merito.

È necessario nominare un Responsabile per la protezione dei dati anche all'interno degli studi legali?

Premesso che non sussiste, in ambito interpretativo, una risposta univoca, né una pronuncia sul punto del Garante che ne specifichi con precisione l'ambito di applicazione, occorre riferirsi a

quanto disposto dall'articolo 37, Regolamento Ue 2016/679.

Dalla lettura della disposizione parrebbe potersi concludere che la necessità o meno della nomina dipenda dal contesto concreto dello studio e dalla relativa attività, indipendentemente dalla propria natura giuridica. In considerazione di detta attività, in particolare, il titolare dello studio sarà chiamato alla nomina di un D.P.O. se per il giro d'affari realizzato e la tipologia di controversie normalmente trattate questi effettui trattamenti che *“richiedono il monitoraggio regolare e sistematico degli interessati su larga scala”* o che riguardino *“categorie particolari di dati personali”*, su larga scala, individuate dallo stesso articolo 37. Appare evidente come il presupposto *“su larga scala”* residui di numerosi margini di incertezza e debba, comunque, ricondursi a più fattori concorrenti, come, a titolo esemplificativo, il numero dei soggetti interessati, il volume e la tipologia dei dati, la portata geografica del trattamento.

Sarà, in ogni caso, sempre possibile nominare, sia internamente che esternamente, un responsabile in maniera volontaria, anche al fine di dimostrare la predisposizione di un modello organizzativo idoneo a prevenire le possibili lesioni alla riservatezza ed evitare le sanzioni che, come si dirà, risultano piuttosto pesanti.

Non v'è dubbio, invero, sulla possibilità per l'avvocato esperto in materia - e per lo studio legale nel suo complesso - di essere nominato responsabile della protezione dei dati presso imprese o studi terzi, anche per mezzo della stipula di un apposito contratto.

Il Registro delle attività del trattamento

Dal dato testuale dell'articolo 30, comma 5 del Regolamento non sembrano esserci dubbi sull'applicabilità agli studi legali dell'obbligo di tenuta del Registro delle attività del trattamento. La norma, infatti, nell'esonerare da tale adempimento le *“imprese o organizzazioni con meno di 250 dipendenti”*, chiarisce altresì che detto obbligo sia comunque sussistente allorquando, nella propria attività, si trattino dati sensibili, con i quali, come sopra rilevato, l'avvocato si ritrova quotidianamente in contatto. Allo stesso tempo, l'esonero non può dirsi operante ove l'impresa o l'organizzazione effettui trattamenti *“non occasionali”*.

Anche gli avvocati, quindi, saranno chiamati alla tenuta del Registro, all'interno del quale dovranno essere indicati puntualmente, a norma del citato articolo 30, l'elenco dei trattamenti posti in essere all'interno dello studio - da aggiornare in maniera costante - accompagnato dallo specifico riferimento alle relative finalità, alle categorie di destinatari, all'eventuale trasferimento di dati, con l'ulteriore previsione di “una descrizione generale delle misure di sicurezza tecniche e organizzative” adottate.

Le sanzioni

Come detto, la necessità di adempiere agli obblighi imposti dal Regolamento Ue 2016/679 assume una particolare rilevanza se si considera che il legislatore europeo ha introdotto, in proposito, un apparato sanzionatorio particolarmente severo, sia con riferimento agli importi sia per le condizioni di irrogazione.

Ebbene, al riguardo, occorre osservare come, a norma dell'art. 83 GDPR, è prevista una sanzione massima di euro 10.000.000 allorquando le violazioni della normativa europea da parte di un soggetto - ivi compresi gli avvocati e gli studi legali - riguardi:

- le prescrizioni relative al consenso del minore;
- le norme sulla certificazione e la sicurezza dei dati personali;
- le norme relative al D.P.O. e al titolare del trattamento dei dati personali;

- le norme sui trattamenti senza identificazione dell'interessato.

Sanzioni ben più rilevanti (fino a 20.000.000) sono, invece, irrogabili in caso di violazione:

- dei principi base del trattamento dei dati personali;
- dei diritti riconosciuti dal Regolamento Ue agli interessati;
- delle norme sul trasferimento dei dati personali in Paesi *extra* Ue e organizzazioni internazionali; di un ordine ovvero di una limitazione operati dall'Autorità di controllo (Garante della privacy). Al citato apparato sanzionatorio si aggiungono, peraltro, le possibili ulteriori sanzioni che, a norma dell'art. 84 GDPR (a mente del quale queste devono risultare “*effettive, proporzionate e dissuasive*”), i singoli Stati Membri possono autonomamente prevedere. Ciò vale, in particolar modo, nell'ambito della tutela penalistica.

Si rileva, da ultimo, che, nell'ambito degli studi legali, a rispondere sarà l'avvocato titolare dello studio legale, allorquando titolare del trattamento. La possibilità di individuare ulteriori responsabili dipenderà dall'eventuale nomina di un responsabile della protezione dei dati. In caso di incarico, infatti, anche il soggetto incaricato sarà chiamato a rispondere, ma solo - ed esclusivamente - ove la specifica violazione di riferimento riguardi le relative attribuzioni e fatta salva la possibilità di liberarsi dimostrando che la violazione non sia allo stesso imputabile.