dente contratto domiciliazione, al proprio commercialista (studio C), dovrà riportare tale circostanza nel contratto di nomina di responsabile del trattamento stipulato con lo studio (A) e ricevere specifica autorizzazione alla nomina dello studio C come *sub* responsabile del trattamento.

Siamo di fronte ad una serie di esempi che ci permettono di delineare il seguente percorso: ogni volta che uno studio trasferisce a soggetti terzi, esterni alla propria organizzazione, al fine di un trattamento esterno, dati di interesse (clienti, dipendenti etc.), dovrà nominare responsabile del trattamento il soggetto al quale trasferisce i dati. Qualora poi quest'ultimo si avvalga, in fase di trattamento, di ulteriori organizzazioni esterne (es: commercialista), dovrà essere indicata nel primo contratto la volontà di avvalersi di un *sub* responsabile del trattamento. La nomina di un *sub* responsabile del trattamento dovrà essere sempre specificatamente autorizzata dal titolare del trattamento.

In tutti i casi descritti, l'atto di nomina dovrà seguire i formalismi richiamati dall'art. 28 del Regolamento. In particolare, il rapporto tra le parti dovrà essere obbligatoriamente documentato con un contratto o altro atto giuridico, con specifica indicazione delle relative responsabilità, anche dirette, nei confronti degli interessati (il titolare e il responsabile, ovvero i responsabili coinvolti nel medesimo trattamento, rispondono in solido per l'intero ammontare del danno cagionato da una eventuale violazione). Inoltre, l'eventuale nomina di *sub* responsabili del trattamento dovrà essere specificatamente autorizzata dal titolare. Quando lo studio professionale opererà quale responsabile del trattamento, dovrà inoltre presentare ga-

LA NOVITÀ NORMATIVA

Responsabile esterno del trattamento

Il responsabile del trattamento non è più un soggetto interno all'organizzazione come avveniva in passato. Oggi, il **responsabile** del trattamento, soggetto esterno all'organizzazione, che tratta dati personali per conto del titolare, tratta i dati forniti da quest'ultimo solo sulla base di **istruzioni** chiare e documentate. Il **contratto di nomina**, nel quale dovrà essere obbligatoriamente indicata l'eventuale volontà di avvalersi di *sub* responsabili del trattamento, apre inoltre lo spazio anche a possibili **audit** da parte del titolare finalizzati a verificare la sussistenza, in capo al responsabile del trattamento, di **garanzie** sufficienti basate sulla messa in atto di **misure tecniche e organizzative** adeguate e in grado di soddisfare i requisiti del Regolamento UE 2016/679.

ranzie professionali sufficienti per attuare misure tecniche e organizzative adeguate. Gli eventuali casi di contitolarità del trattamento sono richiamati dall'art. 26 del Regolamento.

All'interno dello studio professionale, il titolare del trattamento potrà autorizzare propri dipendenti e collaboratori al trattamento dei dati in conformità alle prescrizioni del Regolamento e nel rispetto dei principi di sicurezza del trattamento di cui all'art. 32 dello stesso Regolamento. Il GDPR, al contrario di quanto av-

veniva nel T.U. *privacy*, non prevede espressamente la figura dell'incaricato al trattamento, quale soggetto che tratta dati operando sotto l'autorità del titolare e del responsabile, tuttavia non esclude la nomina di un soggetto con tali caratteristiche.

L'adeguatezza delle misure di sicurezza all'interno dello studio professionale

In passato l'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza) del D.Lgs. n. 196/2003 forniva specifiche indicazioni circa le azioni da implementare, all'interno del proprio studio, per rispettare le c.d. misure minime di sicurezza. Tali misure erano basate, sostanzialmente, su procedure di autenticazione, autorizzazione e su altre misure generali.

L'introduzione del Regolamento UE ha indotto alcuni operatori ad ipotizzare, in modo erroneo, che l'intervenuta inefficacia del richiamato allegato B potesse comportare la contestuale eliminazione delle misure minime di sicurezza all'interno delle organizzazioni e quindi anche degli studi professionali. L'interpretazione non è corretta, in quanto la dimostrazione della conformità dell'organizzazione, nel trattamento

dei dati personali, alla nuova disciplina regolamentare passa, oggi come ieri, anche per l'implementazione di misure tecniche ed organizzative che siano adeguate, ma soprattutto disegnate, sulle specifiche caratteristiche dell'organizzazione di riferimento. In pratica, l'art. 32 del GDPR, che richiama fedelmente la logica della responsabilizzazione, impone, anche per gli studi professionali, l'attuazione di misure tecniche e orga-

nizzative adeguate per garantire un livello di sicurezza conforme al Regolamento UE, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura dell'oggetto, del contesto e delle finalità del trattamento. Spetta quindi al titolare del trattamento definire autonomamente quali siano le misure idonee per la propria organizzazione. In ogni caso, ad opinione di chi scrive, soprattutto nelle strutture di piccole dimensioni, quali di norma sono gli studi professionali, lo schema proposto in passato dell'allegato B può ancora rappresentare un primo strumento di lettura e di approfondimento nella selezione e successiva implementazione di misure adeguate.

L'adozione del registro dei trattamenti

Gli studi professionali italiani, tranne poche eccezioni, hanno un numero di dipendenti inferiore a 250. Questa soglia relativa ai dipendenti rappresenta uno dei limiti dimensionali al superamento del quale vige l'obbligo di tenuta del registro. Tuttavia, è importante ricordare che il comma 5 dell'art. 30 del Regolamento impone la tenuta del registro anche alle organizzazioni più piccole, ma che trattino dati che presentino un rischio per i diritti e le libertà dell'interessato o che includano le categorie particolari di dati personali di cui agli

LA NOVITÀ NORMATIVA

Sicurezza del trattamento

L'art. 32 del GDPR propone una chiave di lettura diversa rispetto al recente passato, finalizzata ad una **responsabilizzazione dell'organizzazione** nella scelta delle misure tecniche e organizzative di **trattamento e protezione dei dati** personali. Lo stesso articolo sottolinea anche la possibilità di dimostrare la conformità ai requisiti attraverso l'adesione ad un **codice di condotta** (art. 40) e/o un **meccanismo di certificazione** (art. 42). Oggi, tuttavia, ancora nessuna certificazione può dichiarare la conformità al GDPR ai sensi degli artt. 42 e 43 del GDPR fino al rilascio delle modalità di accreditamento.

art. 9 e 10 del Regolamento. Pertanto, in via esemplificativa, il mero trattamento di dati relativi alla salute o all'appartenenza sindacale, frequenti in presenza di dipendenti, impone, in linea di principio, la tenuta del registro dei trattamenti anche agli studi professionali. Recentemente, il 19 aprile 2018, il gruppo di lavoro *ex art. 29* ha emanato un documento interpretativo riferito all'art. 30, comma 5 (3). Il documento preci-

sa l'alternatività delle condizioni di esenzione dalla tenuta del registro elencate precedentemente e, soprattutto, specifica che le organizzazioni rientranti per caratteristiche in quelle tipiche di uno studio professionale (meno di 250 dipendenti e trattamenti *ex art. 9* molto circoscritti) possono adottare alcune misure di semplificazione, potendo limitare la redazione del registro unicamente alle attività a rischio (si tratta di quelle richiamate dagli artt. 9 e 10 Regolamento). In particolare, qualora il rischio sia limitato alla presenza di categorie particolari di dati legati alla gestione, ad esempio, di pochissimi dipendenti, il registro si riferirà esclusivamente a tale tipologia di trattamento. Il registro, quando prescritto, deve essere redatto in forma scritta, anche su formato elettronico, e su richiesta deve essere posto a disposizione dell'Autorità di controllo. Questo strumento permette di dimostrare la capacità del titolare e del responsabile (se nominato) di conformarsi al GDPR e di conservare in maniera ordinata, ricostruibile *ex post* e verificabile da terzi, le considerazioni svolte in merito alla mappatura ed analisi di tutti i trattamenti attuati dall'organizzazione. Il registro dimostra, altresì, l'adozione di misure adeguate ed efficaci volte ad attuare la piena *compliance* al GDPR. Da qui nasce l'invito generale dell'Au-

(3) Art. 29 WP, *position paper related to article 30(5)*.

torità garante, rivolto a tutte le organizzazioni, all'adozione del registro indipendentemente da un obbligo specifico.

In conclusione, è opportuno richiamare integralmente tutti gli ulteriori aspetti del Regolamento UE 2016/679 che in ogni caso incidono sull'organizzazione dello studio professionale. In particolare si ricorda l'art. 17, in riferimento al c.d. diritto all'oblio, che estende il diritto di cancellazione dei dati degli interessati già previsto nelle precedenti normative, il principio

della data *portability* e quello relativo al *data breach notification*. Questi ultimi sanciscono rispettivamente il diritto dell'interessato di ricevere dal titolare del trattamento in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e il contestuale diritto di trasmettere tali dati a un altro titolare del trattamento, senza impedimenti da parte del precedente titolare del trattamento e, nel caso del *data breach notification*, la previsione che, in caso di violazione dei dati personali, il titolare effettui una notifica dell'accaduto agli interessati e all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a me-

LA NOVITÀ NORMATIVA

Registro dei trattamenti

Il registro dei trattamenti rappresenta una delle novità di maggiore rilievo. È lo strumento chiave per la dimostrazione del rispetto del **principio di responsabilizzazione**. Gli studi professionali sono obbligati alla tenuta del registro solo se hanno un **numero elevato di dipendenti** (oltre 250) o in presenza di trattamento di **dati particolari** di cui agli artt. 9 e 10 del GDPR e con riferimento esclusivo a **tali tipologie** di trattamento. Tuttavia, l'Autorità garante per la privacy ha auspicato, all'interno delle raccomandazioni delle linee guida al Regolamento, l'adozione di questo strumento per tutte le organizzazioni, ritenendo la tenuta del registro dei trattamenti parte integrante di un sistema di corretta gestione dei dati personali.

no che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

Infine, in riferimento all'esigenza di nomina del DPO (*Data Protection Officer* o Responsabile della protezione dei dati), l'Autorità garante per la privacy ha chiarito espressamente che non è necessaria tale nomina "in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale". Per gli studi associati la valutazione sulla nomina di tale figura dovrà essere legata alla di-

mensione e tipologia di dati trattati, all'eventuale presenza di un monitoraggio regolare e sistematico degli interessati su larga scala o basata sulla presenza di trattamenti, sempre su larga scala, di dati "sensibili".

Lo studio professionale è quindi assoggettato a tutti gli effetti agli obblighi sanciti dal GDPR. L'adeguamento alle norme in esso sancite aggiunge, ad un'azione di *compliance* organizzativa, un forte valore deontologico soprattutto in riferimento, in particolare, ai principi di trasparenza (Capo III, art. 12), di informazione all'interessato (Capo III, artt. 13-14) e di comunicazione dei diritti dell'interessato (Capo III, artt. 15, 16, 17, 18, 20, 21) sanciti dal Regolamento UE 2016/679.

La privacy nello studio professionale

di Tommaso D'Onofrio

Il 25 maggio 2018 il **Regolamento UE 2016/679** in materia di protezione dei dati personali ha manifestato i suoi **effetti**, in ambito UE, nei confronti di tutte le **organizzazioni** che trattano **dati personali** relativi a persone fisiche. All'interno della generica definizione di "organizzazione", vengono ricompresi anche gli **studi professionali** e i **singoli professionisti** operanti in forma individuale. Il Regolamento in questione, per la sua natura giuridica, non deve essere recepito all'interno dell'ordinamento nazionale e di conseguenza l'attuale assenza in Italia di un decreto ad hoc (il nostro legislatore dovrà procedere con l'emanazione di un decreto entro il 21 agosto 2018) non produce alcuna proroga degli effetti, anche sanzionatori, sugli operatori nazionali. Dal 25 maggio scorso, pertanto, anche gli **esercenti** le libere **professioni** sono tenuti a porre in essere **misure e procedure** idonee per un trattamento ed una protezione dei dati personali conformi al predetto Regolamento.

In un precedente intervento (1), ci siamo soffermati sugli effetti del Regolamento UE 2016/679 in materia di protezione dei dati personali (di seguito, "Regolamento" o "GDPR"), che sostanzialmente rivoluziona l'approccio alla *privacy* in ambito comunitario. Tutte le norme e i principi richiamati all'interno di quell'articolo sono applicabili anche alle organizzazioni di tipo professionale (d'ora in avanti anche "studio") operanti sia in forma individuale che associata. In questo approfondimento, proveremo a focalizzare l'attenzione sugli adempimenti ai quali, trasversalmente, possono essere assoggettati tutti i liberi professionisti in forma individuale o associata.

È ormai chiaro che si è passati da un sistema basato su un modello autorizzatorio ad una nuova visione orientata all'introduzione di un nuovo principio-chiave, quella della *responsabilizzazione* (*accountability*). Ciò impone di disegnare il sistema *privacy* del proprio studio professionale considerandone le specifiche caratteristiche e peculiarità, attraverso l'implementazione di misure tecniche ed organizzative adeguate e con l'approccio tipico dei sistemi di gestione.

Bisogna, inoltre, considerare che, all'interno dell'ampia accezione di professionista, si collocano categorie ampie e diversificate e ciò ren-

de non sempre agevole la descrizione di un percorso omogeneo di azioni per la conformità dello studio alla nuova disciplina regolamentare. Tuttavia, pur nelle descritte diversità dimensionali e di appartenenza categoriale dei singoli studi, alcuni passaggi chiave possono essere sicuramente focalizzati in modo trasversale.

La condivisione dell'informativa

Uno dei primi adempimenti che lo studio dovrà porre in essere nel trattare i dati personali dei propri clienti, fornitori, dipendenti e più in generale, in ogni trattamento di dati personali, è correlato all'obbligo di rilasciare un'informativa concisa, trasparente, intellegibile, facilmente accessibile e con un linguaggio semplice e chiaro. L'informativa, qualora i dati personali siano stati raccolti presso l'interessato (questo è il caso più comune all'interno degli studi professionali), richiamerà in intestazione l'art. 13 del Regolamento UE 2016/679, in alternativa, nel caso in cui i dati non siano stati ottenuti presso l'interessato, si farà riferimento all'art. 14 dello stesso Regolamento. La lettura approfondita dei predetti due articoli fornisce un quadro completo del contenuto dell'informativa che per tutti gli operatori deve essere considerato, nella sua chiara elencazione, asso-

(1) Cfr. T. D'Onofrio e C. Macculi, "La rivoluzione GDPR", in *Corr. Trib.*, n. 23/2018, pag. 1838.

lutamente tassativo. Talvolta, all'interno di alcune informative *privacy* rilasciate dagli studi professionali, è possibile ancora ritrovare il richiamo al TU *privacy* (D.Lgs. n. 196/2003). È bene ricordare che, attualmente, gli articoli del D.Lgs. n. 196/2003, ove in contrasto con le disposizioni del Regolamento UE, sono inefficaci. Tra questi articoli, ormai inefficaci, vi è certamente da considerare anche l'art. 13 del D.Lgs. n. 196/2003. Per tale ragione, oggi, l'inserimento,

anche di un mero richiamo, al predetto art. 13 del D.Lgs. n. 196/2003 non ha alcun senso e pertanto va del tutto evitato. Per completezza è opportuno precisare che l'art. 13 del Regolamento UE tratta delle informative (di cui l'interessato deve prendere visione) e non dei consensi (per i quali l'interessato, nei casi previsti, deve prestare autorizzazione). La differenza è apparentemente sottile, ma sostanziale. Troppo spesso le informative rilasciate dagli studi si concludono con una superflua richiesta di "autorizzazione" al trattamento dei dati personali. Un'attestazione di presa visione formale dell'informativa può essere importante al fine di ricostruire *ex post* l'avvenuto rilascio della stessa, ma non deve essere confusa con la prestazione di un consenso.

I trattamenti effettuati all'esterno per conto del Titolare

Un secondo adempimento che trasversalmente tocca tutte le strutture professionali riguarda il ricorso, richiamato dall'art. 28 del Regolamento UE 2016/679, al c.d. responsabile del trattamento. Come già chiarito in un precedente intervento (2), il responsabile del trattamento è un soggetto esterno all'organizzazione che tratta i

LA NOVITÀ NORMATIVA

Informativa

Rispetto alla precedente normativa, l'informativa assume contenuti più ampi, sia alla luce della nascita di nuovi **diritti per l'interessato** e di nuove **figure professionali** in ambito *privacy* (i dati di contatto del Data Protection Officer vanno appunto indicati nell'informativa), sia in considerazione dell'introduzione di nuovi **elementi obbligatori**, tra i quali l'inserimento del **periodo di conservazione dei dati**. Tali modifiche impongono agli studi professionali una radicale rilettura anche delle informative precedentemente rilasciate, con l'obbligo di condivisione con gli interessati di una nuova informativa contenente tutti gli elementi tassativamente elencati all'interno del Regolamento.

dati per conto del titolare. All'interno di uno studio professionale la fattispecie ivi richiamata potrebbe porre lo stesso studio in una duplice situazione: passiva (nomina dello studio quale responsabile del trattamento da parte di un terzo titolare) o attiva (lo studio professionale, titolare del trattamento, attribuisce contrattualmente ad un terzo la qualifica di responsabile del trattamento).

Il primo caso potrebbe configurarsi, ad esempio, allorché uno studio legale riceva l'incarico di

mandatario da un altro studio legale. Un cliente dello studio legale ("interessato" in linguaggio di *privacy*) potrebbe, difatti, avere affidato un incarico ad un legale di sua fiducia ma, dovendosi esperire l'azione in un'altra città, quest'ultimo potrebbe, tipico caso di domiciliazione, avvalersi dell'ausilio di un collega appartenente al foro competente per lo svolgimento della causa. Al verificarsi di tale ipotesi, lo studio legale che ha ricevuto l'incarico in qualità di titolare del trattamento (studio A) dovrà nominare responsabile del trattamento dei dati relativi al proprio cliente il secondo studio legale (studio B) domiciliato nel luogo nel quale viene esperita la causa. In questo caso lo studio B opererebbe come responsabile del trattamento. Lo stesso studio B potrebbe avere la necessità di avvalersi di un commercialista (studio C) per la tenuta della propria contabilità; in questo caso, considerando l'esigenza di trasferire i dati personali dei propri clienti al proprio professionista contabile di fiducia, dovrà procedere, operando nel contratto come titolare del trattamento, alla nomina di quest'ultimo quale responsabile del trattamento. Inoltre, qualora lo studio B trasferisca i dati personali dei clienti dello studio (A), ricevuti in virtù del prece-

(2) Cfr. nota 1.