Ordine degli
Avvocati di Milano


# VADEMECUM PER GLI AVVOCATI
## *COME GESTIRE LA PRIVACY*

QUADERNI DELL'ORDINE N. 8 / MILANO 2018

# VADEMECUM PER GLI AVVOCATI
# COME GESTIRE LA PRIVACY

## ☑ 1 - Introduzione

Il quadro normativo europeo applicabile alla tutela dei dati personali è stato oggetto di una crescente produzione normativa che ha portato dall'adozione della direttiva 95/46/EC (*Privacy Directive*) alla definizione in via giurisprudenziale di principi generali, fino al riconoscimento del diritto di disporre dei propri dati personali come diritto fondamentale della persona sancito dal diritto primario all'art. 16 del Trattato sul funzionamento dell'UE (TFUE) e dall'art. 8 della Carta dei diritti fondamentali.

L'entrata in vigore del Trattato di Lisbona nel 2009, sancendo espressamente la vincolatività della Carta, ha provveduto a chiarire definitivamente la base giuridica vincolante per la tutela dei dati personali in qualità di diritto fondamentale. La protezione offerta dal diritto europeo ai diritti fondamentali è stata progressivamente ampliata dalla giurisprudenza europea traendo spunto dalle tradizioni costituzionali comuni degli Stati membri.

Il diritto alla protezione dei propri dati personali, benché qualificato come diritto fondamentale della persona, deve essere bilanciato con gli altri diritti fondamentali e, in particolare, con il diritto all'informazione e alla trasparenza. Proprio nel procedere alla valutazione, caso per caso, del bilanciamento d'interessi è fondamentale la guida fornita dall'interpretazione della Corte di vertice del sistema europeo. Tuttavia, è essenziale, nel definire il quadro generale, non trascurare il ruolo fondamentale che il giudice nazionale assolve nell'applicare il diritto dell'Unione, al fine di attuarlo e garantire che la protezione sancita in via teorica possa diventare strumento concreto di diritto nelle aule di giustizia di tutto il territorio dell'Unione.

## ☑ 2 - Novità normative nel panorama europeo

Nel gennaio 2012 la Commissione europea ha ufficialmente presentato il c.d. "pacchetto protezione dati" con lo scopo di garantire un quadro coerente e un sistema complessivamente armonizzato nell'Unione. Tale pacchetto era composto da due strumenti legislativi: una proposta di regolamento concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, volta a disciplinare i trattamenti di dati personali sia nel settore privato sia nel settore pubblico, e destinata a sostituire la Direttiva 95/46; una proposta di direttiva indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali, che sostituirà e integrerà la decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia.

Il 4 maggio 2016, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) i testi del Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini. Il 5 maggio 2016 è entrata ufficialmente in vigore la Direttiva, che dovrà essere recepita dagli Stati membri entro 2 anni. Il 24 maggio 2016 è entrato ufficialmente in vigore il Regolamento, che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Il regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue, e per i casi di violazione dei dati personali (*data breach*).

Pertanto, con l'adozione del GDPR che garantisce l'evoluzione dal diritto alla *privacy* al diritto di disporre dei propri dati personali, l'Unione ha completato il panorama legislativo, aggiornandolo alla realtà dei *social network* e dei motori di ricerca, e qualificandolo come uno dei più sofisticati sistemi di protezione nel mondo. Un regolamento era lo strumento giuridico necessario per garantire un livello di pro-

tezione coerente, per evitare divergenze nella legislazione nazionale e per attuare la libera circolazione nel mercato interno. Infine, solo l'adozione del regolamento garantisce alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti, giuridicamente vincolanti per i soggetti interessati, nonché gli stessi obblighi, responsabilità e sanzioni equivalenti per coloro che processano i dati.

## ☑ 3 - L'avvocato e la Privacy

Ogni avvocato svolgendo la propria attività professionale quotidiana tratta dati personali, dall'analisi di una richiesta all'incontro con un cliente fino alla richiesta del pagamento dei propri onorari, diventando così titolare del trattamento dei dati personali che processa.

La direttiva 95/46 necessitava di essere trasposta negli ordinamenti giuridici nazionali. In Italia l'adeguamento normativo all'obbligazione internazionale è stato sancito dal decreto legislativo 196 del 30 giugno 2003 che istituisce il Codice in materia di protezione dei dati personali (Codice *Privacy*). Il Codice *privacy* del 2003 nasce quindi da una primaria esigenza di riordino della materia, ma anche dalla necessità di sistematizzare e cristallizzare in un testo normativo le interpretazioni delle pronunce del Garante. La disciplina in vigore con il Codice è stata successivamente integrata da pronunce successive del Garante. Il diritto alla protezione dei dati personali, così come i diritti della personalità, tutelano il medesimo bene giuridico ossia l'identità dell'individuo declinata nei suoi molteplici aspetti.

Con l'approssimarsi della piena e diretta applicabilità del nuovo regolamento europeo in materia di protezione di dati personali – regolamento 679/2016 – pubblicato sulla Gazzetta ufficiale dell'Unione Europea (GUUE) nel maggio 2016, si è ritenuto opportuno provvedere a diffondere alcuni elementi fondamentali che regolano la materia e riflette sul ruolo degli avvocati nel tutelare il diritto fondamentale alla riservatezza conformemente con le disposizioni deontologiche.

È necessario che gli avvocati nello svolgimento della professione siano consapevoli della tutela da garantire agli aventi diritto (*data*

*subjects*), ma anche quali sono le sanzioni, attualmente inasprite dal regolamento, per effettuare una valutazione del rischio e una gestione, opportunamente modellata, della *privacy* nei propri studi legali.

La Legge di delegazione europea 2017 conteneva delega al Governo per l'adozione entro sei mesi di uno o più decreti legislativi al fine di adeguare il quadro normativo al regolamento nel rispetto dei seguenti principi e criteri: abrogare espressamente le disposizioni del Codice *Privacy* incompatibili con il regolamento; modificare il Codice *Privacy* e successive modificazioni, limitatamente a quanto necessario; coordinare le disposizioni vigenti con le disposizioni del regolamento; prevedere il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante nell'ambito e per le finalità previste dal regolamento; adeguare, nell'ambito delle modifiche al Codice *Privacy*, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione.

È necessario che il legislatore italiano intervenga prontamente e puntualmente a definire il coordinamento tra le disposizioni nazionali e il regolamento europeo al fine di garantire certezza giuridica circa le disposizione del Codice *Privacy* da considerarsi in vigore e quelle abrogate.

## ☑ 4 - L'Ordine degli Avvocati di Milano e la Privacy

Il regolamento invita associazioni e organizzazioni a elaborare codici di condotta nei limiti del regolamento, in modo da facilitarne l'effettiva applicazione. Ovviamente tali elaborazioni devono tenere conto delle caratteristiche specifiche dei trattamenti effettuati nei diversi settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese. In particolare, tali codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento e dei responsabili del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche.

Obiettivo dell'Ordine degli Avvocati di Milano è l'elaborazione, eventualmente in concerto con il Consiglio Nazionale Forense, di un progetto di codice di condotta da sottoporre alla valutazione del Garante Italiano per la Privacy che formulerà parere sulla conformità del progetto al regolamento europeo e approverà tale progetto se reputa che offra garanzie adeguate per gli utenti. L'adesione e l'applicazione di un codice di condotta già approvato dovrebbe contribuire a una semplificazione, garantire specialmente certezza del diritto, per gli avvocati titolari del trattamento che devono effettuare la valutazione del rischio.

Considerato che la *privacy* s'interseca con molti aspetti dell'attività amministrativa dell'Ordine e, come analizzato, è un diritto fondamentale che deve essere bilanciato con altri diritti contrapposti, si reputa opportuno fornire le seguenti informazioni circa due regolamenti del Consiglio dell'Ordine di recente produzione che esplicano il bilanciamento tra *privacy* e pubblicità. Il primo è inerente il diritto di accesso ai documenti amministrativi. Tale diritto è esercitabile fino a quando il Consiglio dell'Ordine abbia l'obbligo di conservare le informazioni, i dati e i documenti amministrativi ai quali si chiede di accedere. È formato e tenuto un registro informatico delle domande di accesso agli atti, distinto per tipologie e riportante i dati dell'esercizio dell'accesso, nonché gli estremi dell'avvenuto rilascio, dell'atto di differimento o di diniego e le eventuali somme riscosse. Il secondo attiene invece il regolamento per l'opinamento e il rilascio del parere di congruità dei compensi relativi ad attività professionale forense. Ai sensi del presente regolamento il contro interessato verrà informato da parte del Consiglio dell'Ordine del procedimento in corso.

## ☑ 5 - Qualche definizione

Le definizioni rilevanti contenute all'art. 4 del regolamento prevedono innanzitutto quella di **dato personale** ovvero *qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato). Si considera identificabile la persona fisica che può essere*

*identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*.

Il diritto alla protezione dei dati personali, anche in considerazione dell'inquadramento di tale diritto come diritto fondamentale, è limitato alle persone fisiche e attualmente la giurisprudenza non ha reputato di estenderlo alle persone giuridiche per evitare contrasti con il principio di trasparenza e certezza.

Vi sono poi **particolari categorie di dati** che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, politiche o filosofiche, l'appartenenza sindacale nonché il trattamento di dati relativi alla salute e alla vita sessuale dell'individuo. L'elencazione tassativa viene invece qualificata nella categoria di "dati sensibili" dal Codice Privacy. E' necessario porre particolare attenzione nel trattamento di dati personali aventi ad oggetto la categoria dei dati sensibili nei quali è evidente la rischiosità intrinseca del trattamento.

Il regolamento fornisce le definizione di "**dati genetici**", "**dati biometrici**" e "**dati relativi alla salute**" ai quali attribuisce autonoma attenzione con particolare riferimento all'acquisizione del consenso dell'interessato. I primi sono quei *dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute della persona fisica, e che risultano in particolare dall'analisi di un campione biologico del soggetto*. I dati biometrici sono *quei dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*. Infine, i dati relativi alla salute sono tutti i *dati personali attinenti alla salute fisica o mentale, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative allo stato di salute*. Benché la natura dei dati sensibili determini l'appartenenza a una categoria chiusa, tuttavia la formulazione del regolamento, così come già nella norma preesistente, attraverso il criterio della riferibili-

tà determina una certa flessibilità nell'applicazione al singolo caso.

Le attività oggetto del regolamento si riferiscono al **trattamento** dei dati personali come sopra definiti. Il trattamento è *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*. La definizione di trattamento comprende quindi qualsiasi operazione, automatizzata o non, effettuata sui dati.

## ☑ 6 - I principi

### *Liceità e correttezza*

Il trattamento deve avvenire in maniera lecita e corretta, informando l'interessato circa la raccolta, l'utilizzo e altri eventuali successivi trattamenti dei dati forniti. Perché sia lecito, il trattamento di dati personali deve fondarsi sul consenso dell'interessato o su altra base giuridica prevista come obbligatoria dal regolamento o dalla normativa europea o da quella statale.

### *Trasparenza*

Al fine di essere trasparente il trattamento deve avvenire con modalità predefinite e rese note all'interessato che sarà quindi pienamente consapevole non solo della tipologia di dati raccolti, ma anche delle modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i suoi dati personali. La trasparenza attiene non solo al contenuto delle informazioni, ma anche alla modalità con cui tali informazioni sono fornite all'interessato.

***Finalità***

Il principio di finalità prevede che vi sia una corrispondenza tra quanto dichiarato dal titolare del trattamento e quanto effettivamente eseguito nell'utilizzo dei dati. Pertanto, i dati personali raccolti e utilizzati dovrebbero essere adeguati, pertinenti e, soprattutto, limitati a quanto necessario per le finalità del trattamento dichiarato. L'esplicitazione delle finalità deve essere antecedente all'acquisizione del consenso poiché solo avvenendo in un momento anteriore all'effettivo inizio del trattamento è possibile garantire che il consenso dell'avente diritto sia effettivamente informato.

***Accuratezza***

Sulla base del principio di accuratezza, il titolare del trattamento, in continuità con quanto già previsto dalla direttiva, deve verificare che i dati siano corretti, veritieri e completi. Il titolare deve trattare dati esatti e deve organizzare la propria struttura aziendale al fine di garantire il controllo sulla veridicità. Sostanzialmente il titolare è gravato dell'obbligo di garantire un elevato *standard* di qualità dei dati.

Il trattamento di dati personali inesatti o incompleti può determinare una falsa rappresentazione dell'individuo interessato che potrebbe subirne conseguenze pregiudizievoli, per esempio la mancata attribuzione di titoli e qualifiche legate all'esercizio della professione.

***Necessità e minimizzazione***

Il principio di necessità prevede che non vi sia alcuna eccedenza nei trattamenti di dati. Quindi, si sostanzia in un trattamento vincolato necessariamente alle finalità dichiarate dal titolare nell'informativa. Saranno pertanto raccolti solo quei dati la cui pertinenza attiene al profilo quantitativo della raccolta.

Nell'effettuare il trattamento con strumenti automatizzati, il titolare dovrà preferire l'utilizzo di dati anonimi rispetto al trattamento di dati personali che dovranno invece essere oggetto del trattamento solo qualora vi sia la necessità d'identificare l'interessato. In applicazione di questo principio i programmi informatici devono essere configurati per preferire l'utilizzo di dati anonimi. Per esempio, il titolare dovrà

sempre preferire il trattamento di dati effettuato mediante l'impiego di codici senza identificazione diretta dell'interessato.

***Integrità e confidenzialità***

Il titolare del trattamento deve adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedirne l'accesso o l'utilizzo non autorizzato. Uno degli elementi fondamentali è l'adozione di adeguate misure di sicurezza intese come per esempio le *password*, la pseudonimizzazione e la cifratura.

***Limitazione all'archiviazione***

La conservazione sia effettuata solo per il tempo strettamente necessario agli scopi stabiliti nelle finalità del trattamento. Tuttavia, è opportuno considerare anche il tempo del quale il titolare ha bisogno per adempiere ai propri obblighi di legge, come per esempio quelli afferenti alla materia tributaria e fiscale o quelli in materia di diritto del lavoro.

## ☑ 7 - L'acquisizione del consenso

Il consenso dell'interessato è uno dei meccanismi predisposti dal legislatore per bilanciare gli interessi contrapposti: da un lato quello di riservatezza del singolo, dall'altro quello al trattamento da parte del responsabile. La manifestazione del consenso costituisce l'incontro tra la libertà personale individuale e quella informativa.

Le condizioni di liceità del trattamento, a cui il consenso dell'interessato appartiene, operano come presupposti che legittimano il titolare a effettuare le attività di trattamento.

Il consenso deve essere espresso in modo inequivoco; viene quindi esclusa ogni forma di consenso tacito, inclusa l'impossibilità per il titolare del trattamento di operare con opzioni già pre-selezionate: "*Se il consenso dell'interessato è prestato nel contesto di una dichiarazione*

*scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro*".

Il consenso deve essere libero e informato. Prima di esprimere il proprio consenso l'interessato è pertanto informato delle modalità di trattamento, delle finalità e dei propri diritti.

Nell'informativa sono presenti tutte le informazioni essenziali all'esercizio dei diritti dell'interessato, come per esempio le informazioni di contatto del titolare e l'indirizzo di posta elettronica per le comunicazioni che facilitino l'esercizio dei diritti e di una eventuale revoca del consenso. L'informativa deve essere precisa e dettagliata quanto alle finalità per cui viene posto in essere il trattamento. Qualora le finalità del titolare venissero modificate nel tempo sarà necessario provvedere alla modifica dell'informativa e all'acquisizione di un nuovo consenso. Sostanzialmente informativa e consenso costituiscono un unico binomio poiché il secondo trae le sue radici dal primo.

Il consenso deve essere specifico, riferirsi a un preciso trattamento, non generico, estendibile a vari possibili trattamenti.

## ☑ 8 - Cosa deve fare l'avvocato in vista dell'entrata in vigore del regolamento europeo sulla privacy?

In applicazione del principio di *accountability*, l'avvocato in qualità di titolare del trattamento dei dati personali, è responsabile delle attività di trattamento. Egli deve quindi garantire che tali attività rispettino i principi generali del regolamento e deve predisporre misure adeguate ed efficaci per garantire la sicurezza dei dati.

Non è più sufficiente limitarsi a effettuare un trattamento lecito, che sia quindi fondato su idonea base giuridica, è necessario anche essere responsabili per quel trattamento.

La responsabilità che grava sul titolare inizia con l'elaborazione del servizio, con la definizione del processo per il trattamento dei dati e procede con la definizione di misure di sicurezza rilevanti e sempre

aggiornate, per culminare con le responsabilità per l'archiviazione dei dati. Il principio di responsabilità impone non solo l'obbligo di dimostrare alle autorità l'attuazione del regolamento, ma anche il raggiungimento di risultati concreti.

Il principio di *accountability* richiede l'adozione di appropriate misure *ex ante*, nella fase di elaborazione e predisposizione dei processi, ma anche delle regolari verifiche *ex post* per controllare la tenuta del sistema.

Con l'entrata in vigore del regolamento 679/2016 la *compliance* sarà un processo da garantire fin dall'albore del pensiero imprenditoriale di un servizio o, comunque, di un processo che veda coinvolto il trattamento di dati personali. La tutela della *privacy*, direttamente incorporata nel progetto, deve essere l'impostazione generale e deve essere vagliata da personale qualificato preposto, così che eventuali problemi si possano prevedere limitando i rischi per gli individui.

## ☑ 9 - Registri delle attività di trattamento

Il titolare ha l'obbligo di tenere un registro delle attività di trattamento che vengono espletate sotto la propria responsabilità. L'obbligo di avere tale documentazione è derogato per le aziende con meno di 250 dipendenti che trattino dati in maniera occasionale e comunque senza particolari livelli di rischio.

Lo strumento costituisce una sorta di mappatura delle procedure interne di ogni titolare che gli consente di avere sotto controllo le finalità per le quali i trattamenti vengono svolti e sviluppare la successiva valutazione di rischio. È necessario come adempimento logico e operativo prima che giuridico, perché il soggetto attivo del trattamento – che ne è responsabile – riesce così a censire con precisione tutte le banche dati e altri elementi rilevanti per la valutazione del rischio.

Il registro costituisce un adempimento da effettuarsi *ex ante*, prima quindi dell'inizio del trattamento. Il registro deve necessariamente contenere i dettagli inerenti le finalità del trattamento, le categorie di soggetti interessati, le tipologie di dati e gli eventuali trasferimenti in Paesi terzi.

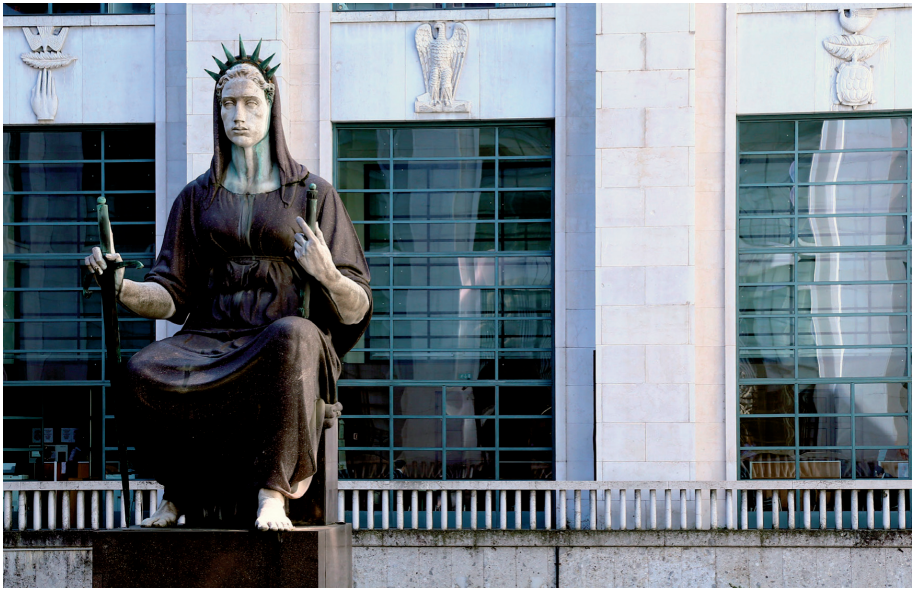
***Privacy Impact Assesment***

È una descrizione sistematica dei processi e dei trattamenti, delle finalità e dell'indicazione dell'interesse legittimo perseguito con il trattamento. La valutazione deve essere svolta avendo riguardo in particolare ai principi di necessità e proporzionalità.

## ☑ 10 – Sanzioni

Il profilo sanzionatorio è uno degli aspetti di maggior rinnovamento della disciplina. Il legislatore italiano con l'adozione del Codice *Privacy* aveva scelto l'impostazione della sanzione amministrativa con previsione addizionale di quella penale per le ipotesi più gravi, quali il trattamento illecito e la mancata previsione di misure di sicurezza, la falsità nelle dichiarazioni al Garante e l'inosservanza dei suoi provvedimenti.

La riforma del profilo sanzionatorio emerge nel regolamento per l'adozione di sanzioni amministrative in percentuale rispetto al fatturato dell'impresa o del gruppo nel caso in cui l'impresa vi appartenga: dal 2% al 4% del fatturato globale.



ORDINE DEGLI
AVVOCATI DI MILANO

OPEN Dot Com

Il ***Gruppo Dot Com*** nasce nel 1999 per creare software e servizi telematici utili nello svolgimento delle professioni ordinistiche, in particolare quelle di Avvocato e di Commercialista.

Dal settembre 2017 ***OPEN Dot Com*** fornisce, grazie ad uno specifico accordo con l'Ordine, la **Consolle Avvocato®** agli Avvocati di Milano e fornisce un'ampia gamma di strumenti on-line e software ad alto contenuto tecnologico, sviluppati da propri team di esperti, curandone direttamente l'assistenza attraverso Gruppi di Studio dedicati.

Dalla fine del mese di marzo 2018, sono disponibili due nuovi interessanti servizi:

ParcellaAvvocato

la soluzione on-line per la gestione del processo di parcellazione dello studio legale

Privacy GDPR EU

il servizio, specifico per lo studio legale, di consulenza e redazione della documentazione prevista dal nuovo Regolamento Generale sulla Protezione dei Dati.

**Per ulteriori dettagli, si vedano:**
**https://www.tuttopro.it/**
**https://www.opendotcom.it/**
**https://www.facebook.com/opendotcomspa**
**https://www.facebook.com/consolle.avvocato/**

ORDINE DEGLI AVVOCATI DI MILANO
c/o Palazzo di Giustizia, via Freguglia 1 - 20122 Milano
Tel. 02 549292. 1 / Fax 02 54101447 - 02 55181003
www.ordineavvocatimilano.it / www.avvocatipermilano.it