ORDINE AVVOCATI BRESCIA

VADEMECUM PER GLI AVVOCATI
COME GESTIRE LA PRIVACY

VADEMECUM PER GLI AVVOCATI
COME GESTIRE LA PRIVACY

R 1 - Introduzione

A partire dal 25 maggio 2018 sarà direttamente applicabile il Regolamento UE 2016/679 (GDPR), in materia di protezione dei dati personali, che introduce significative novità che interessano imprese e professionisti. Anche gli studi legali ed il singolo avvocato hanno l'obbligo di uniformarsi alla normativa, pena pesanti sanzioni, soprattutto pecuniarie.

In particolare, viene alla luce il principio di responsabilizzazione *(accountability)*, che implica la libertà del titolare del trattamento nell'approntare misure adeguate alla protezione dei dati personali, senza basarsi solamente su modelli precompilati ovvero documentazione standard: dunque, oltre a prevedere delle misure di base (in applicazione del principio denominato *"privacy by default"*), ciascun titolare del trattamento dovrà adottare delle procedure modellate sulle necessità e caratteristiche del trattamento svolto all'interno della propria realtà (*"privacy by design"*).

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.

R 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 protezione 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.

R 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 – re-

golamento 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.

Quando l'avvocato utilizza i dati deve sempre operare le seguenti modalità di utilizzo

finalizzati	I dati devono essere pertinenti a quanto necessario per lo scopo del trattamento dichiarato. L'informazione espressa da parte dell'avvocato delle finalità deve precedere l'acquisizione del consenso affinché quest'ultimo sia effettivamente consapevole.
accurati	Deve esserci una verifica della correttezza, veridicità e completezza dei dati. L'avvocato è tenuto non solo a trattare dati esatti garantendo quindi la loro qualità, ma deve anche approntare una organizzazione che garantisca il relativo controllo con adozione di tutte le misure necessarie alla rettificazione o cancellazione di dati inesatti
limitati	Si devono trattare solo i dati strettamente necessari alle finalità dichiarate nell'informativa.
utilizzati in modo riservato e confidenziale	anche attraverso l'utilizzo di sistemi di sicurezza (cifratura e anonimizzazione attraverso attribuzione di numero riferimento).
conservati (archiviati) non oltre il tempo strettamente necessario	Si devono trattenere i dati solo per il tempo necessario al conseguimento delle finalità del trattamento e per gli obblighi di legge.

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.

Il legislatore italiano ha predisposto uno schema di decreto legislativo volto ad armonizzare la normativa interna con il Regolamento, tuttora in fase di approvazione. Pertanto, le indicazioni nonchè la documentazione che verrà fornita in allegato alla presente potranno subire integrazioni e modifiche.

L'avvocato deve provare il rispetto dei principi applicabili al trattamento dei dati personali, tramite vari adempimenti:

- designazione del DPO, ove previsto dalla legge. La nomina non è obbligatoria per i singoli avvocati, salvo che non si ricada nella lett. c) art. 37 GDPR (come per esempio i "megastudi"), ossia se lo Studio Legale, pur a dimensioni ridotti, tuttavia effettui trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala ovvero tratti, sempre su larga scala, categorie particolari di dati personali (i "dati particolari", sono quei dati qualificati in precedenza come "dati sensibili" o i dati "di carattere giudiziario");
- istituzione del registro delle attività di trattamento, nei casi previsti dall'art. 30 GDPR: esso non compete "*alle imprese o organizzazioni* con meno di 250 dipendenti, *a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.*" L'istituzione e la tenuta del registro, in ogni caso, è fortemente consigliata dal Garante della privacy, perché consente una prima valutazione e diagnosi dei dati trattati all'interno della struttura;

- notifica di eventuali *data breach*, con specifiche procedure da attivare in caso di eventuali violazioni;
- aggiornamento dell'informativa sulla base degli artt. 13 e seguenti GDPR (si veda il modello allegato);
- verifica processi interni allo Studio in tema di trattamento dati, ai sensi dell'art. 24 GDPR, provvedendo a definire in maniera adeguata i ruoli e assicurandosi che tutto il personale riceva adeguata formazione. È per esempio necessario che le pratiche siano archiviate sottochiave e non siano riportati i nomi delle parti sull'esterno del fascicolo qualora questo venga poi lasciato in aree visibili come per esempio le sale riunioni;
- verifica dei sistemi informatici per assicurare il rispetto dei principi di protezione dei dati;
- formalizzare o rinnovare rapporti contrattuali con eventuali responsabili esterni del trattamento dei dati. Si pensi per esempio al commercialista o all'ufficio paghe che ricevono incarico come responsabili esterni del trattamento;
- prevedere nuove specifiche autorizzazioni per i soggetti che trattano i dati, per esempio con l'adozione di livelli di sicurezza distinti in funzione dell'incarico ricoperto;
- verifica sull'adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza proporzionato al rischio;
- verifica sulla necessità di procedere ad una valutazione di impatto privacy (DPIA).

R 4 - L'Ordine degli Avvocati 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 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.

Il Garante della protezione dei dati personali ha dato precise indicazioni agli organismi pubblici indicando la centralità del principio di "responsabilizzazione" (cd. *accountability*), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali, e individuando le priorità fondamentali. L'Ordine degli Avvocati, su indicazione del Consiglio Nazionale Forense, ha provveduto a stabilire una scansione temporale degli adempimenti per l'attuazione della normativa europea con le seguenti azioni:

1. La designazione in tempi stretti del *Data Protection Officer*;
2. L'istituzione del Registro delle attività di trattamento;
3. La notifica degli eventuali *data breach* e l'introduzione di specifiche procedure da attivare a seguito delle eventuali violazioni.

L'Ordine degli Avvocati ha inoltre provveduto a:

- Aggiornare l'informativa che verrà poi pubblicata sul sito *web* dell'Ordine;
- Riesaminare le politiche interne in tema di trattamento di dati personali, provvedendo anche a definire in maniera adeguata i ruoli e assicurarsi che tutti coloro che trattano dati personali ricevano adeguate istruzioni e formazione (ex art. 29 del GDPR);
- Procedere alla verifica dei sistemi informatici, per assicurare il rispetto dei principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita di cui all'art. 25 GDPR (concetti di *privacy-by-default* e *privacy-by-design*);
- Esaminare i rapporti contrattuali con i responsabili esterni del trattamento, per verificarne la conformità (art. 28 del GDPR);
- Verificare l'adozione delle misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del GDPR;
- Valutare se si debba procedere, per uno o più trattamenti, ad effettuare una valutazione d'impatto privacy (art. 35 del GDPR).

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. È 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 riferibilità 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.

R 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.

Per esempio, il pagamento dello stipendio e quindi il trattamento dei dati bancari trova il proprio fondamento giuridico nell'esecuzione del contratto di lavoro. La base per il trattamento è la legge o un contratto o il consenso dell'avente diritto firmato separatamente rispetto al contratto.

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.

Per esempio, non sarà possibile procedere alla creazione della banca dati con utilizzo delle mail dei clienti per l'invio di materiale informativo qualora in precedenza il consenso non sia stato acquisito presso il cliente stesso.

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.

Per esempio, non sarà possibile l'invio di una newsletter dedicata nel caso in cui non sia stato acquisito il consenso presso il cliente stesso.

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.

R 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.

Modello di informativa Privacy

Oggetto:
Informativa ai sensi dell'art. 13 del Regolamento UE n. 2016/679

Ai sensi dell'art. del Regolamento UE n. 2016/679 (di seguito "GDPR 2016/679"), recante disposizioni a tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, desideriamo informarLa che i dati personali da Lei forniti formeranno oggetto di trattamento nel rispetto della normativa sopra richiamata e degli obblighi di riservatezza cui è tenuto il professionista.

Titolare del trattamento
Il Titolare del trattamento è l'Avv. _____,
con Studio sito in _____ V. _____.

Responsabile del trattamento - (eventuale)
Il responsabile del trattamento è _____, Via _____.

Responsabile della protezione dei dati (DPO) - solo se previsto dalla legge
Il responsabile della protezione dei dati (DPO) è _____
Via _____.

Finalità del trattamento
I dati personali da Lei forniti sono necessari per lo svolgimento del rapporto lavorativo e per l'esercizio del diritto di difesa.

Modalità di trattamento e conservazione
Il trattamento sarà svolto in forma automatizzata e/o manuale, nel rispetto di quanto previsto dall'art. 32 del GDPR 2016/679 in materia di misure di sicurezza, ad opera di soggetti appositamente incaricati e in ottemperanza a quanto previsto dall'art. 29 GDPR 2016/ 679.
Le segnaliamo che, nel rispetto dei principi di liceità, limitazione delle finalità e minimizzazione dei dati, ai sensi dell'art. 5 GDPR 2016/679, previo il Suo consenso libero ed esplici-

to espresso in calce alla presente informativa, i Suoi dati personali saranno conservati per il periodo di tempo necessario per il conseguimento delle finalità per le quali sono raccolti e trattati.

Ambito di comunicazione e diffusione
Informiamo inoltre che i dati raccolti non saranno mai diffusi e non saranno oggetto di comunicazione senza Suo esplicito consenso, salvo le comunicazioni necessarie che possono comportare il trasferimento di dati ad enti pubblici, a consulenti o ad altri soggetti per l'adempimento degli obblighi di legge.

Trasferimento dei dati personali
I suoi dati non saranno trasferiti né in Stati membri dell'Unione Europea né in Paesi terzi non appartenenti all'Unione Europea.

Categorie particolari di dati personali
Ai sensi degli articoli 9 e 10 del Regolamento UE n. 2016/679, Lei potrebbe conferire al professionista dati qualificabili come "categorie particolari di dati personali" e cioè quei dati che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". Tali categorie di dati potranno essere trattate solo previo Suo libero ed esplicito consenso, manifestato in forma scritta in calce alla presente informativa.

Diritti dell'interessato
In ogni momento, Lei potrà esercitare, ai sensi degli articoli dal 15 al 22 del Regolamento UE n. 2016/679, il diritto di:

a) chiedere la conferma dell'esistenza o meno di propri dati personali;
b) ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione;
c) ottenere la rettifica e la cancellazione dei dati;
d) ottenere la limitazione del trattamento;
e) ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad un altro titolare del trattamento senza impedimenti;
f) opporsi al trattamento in qualsiasi momento ed anche nel caso di trattamento per finalità di marketing diretto;
g) opporsi ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione.
h) chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
i) revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j) proporre reclamo a un'autorità di controllo.

Può esercitare i Suoi diritti con richiesta scritta inviata a _____, all'indirizzo postale della sede legale o all'indirizzo mail _____.

Io sottoscritto/a dichiaro di aver ricevuto l'informativa che precede.

Luogo, lì _____.

Io sottoscritto/a alla luce dell'informativa ricevuta

o esprimo il consenso o NON esprimo il consenso al trattamento dei miei dati personali inclusi quelli considerati come categorie particolari di dati.
o esprimo il consenso o NON esprimo il consenso alla comunicazione dei miei dati personali d enti pubblici e società di natura privata per le finalità indicate nell'informativa.
o esprimo il consenso o NON esprimo il consenso al trattamento delle categorie particolari dei miei dati personali così come indicati nell'informativa che precede.

R 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.

In conclusione l'avvocato deve: creare un registro delle attività di trattamento, riconsiderare le proprie procedure nelle quali vi è coinvolto il trattamento dei dati personali al fine di garantire la tutela alla riservatezza, aggiornare l'informativa fornita ai clienti, verificare i sistemi informatici e verificare clausole contrattuali e nomine per eventuali responsabili esterni del trattamento dei dati personali. È necessario indicare dove avviene il trattamento dei dati cioè Il trattamento dei dati personali avviene esclusivamente all'interno dello studio sito al _____ piano dell'edificio di Via _____

Indicando le modalità con le quali avviene il trattamento dei dati personali sarà possibile indicare

– Schedari ed altri supporti cartacei

I supporti cartacei, ed altri supporti idonei a conservare dati personali, ivi inclusi quelli contenenti suoni od immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati all'interno di armadi ciascuno dotato di chiusura a chiave.

– Elaboratori non in rete

Per elaboratori non in rete si intendono quelli non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici. Essi sono costituiti da:

- Numero _____ postazioni fisse, dislocate come segue:
  - Stanza Avv. _____;
  - Elaboratori in rete pubblica

I seguenti PC, pur non risultando connessi in rete con altri, dispongono di collegamento ad Internet:

- Numero _____ PC fissi, dislocati come segue:
  - Stanza Avv. _____.

A titolo meramente esemplificativo e non esaustivo gli avvocati sono titolari dei dati personali: dei dipendenti e dei collaboratori; dei clienti; dei fornitori. Inoltre, in funzione dell'ambito giuridico trattato dallo Studio potranno essere trattati dati personali dei minori nel caso del diritto di famiglia o dati inerenti la salute dei lavoratori nel caso del diritto del lavoro o dati inerente la salute della persona nel caso di sinistri e risarcimento del danno.

L'insieme della tipologia dei dati trattati ricomprende pertanto i seguenti dati comuni, sensibili e giudiziari relativi a clienti / fornitori / consulenti / personale amministrativo / collaboratori / praticanti:

- dati comuni dei clienti, dei fornitori e di terzi ricavati da albi, elenchi pubblici, visure camerali e di fonti analoghe;
- dati comuni del personale dipendente, collaboratori e praticanti necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, dati richiesti ai fini fiscali, previdenziali, e di natura bancaria e postale;
- dati comuni dei clienti, o dei loro familiari, dagli stessi forniti per l'espletamento degli incarichi affidati allo studio e necessari per l'espletamento di ogni tipo di attività di tutela giudiziaria, compresi i dati sul patrimonio e sulla situazione economica, necessari per fini fiscali, redazione istanze ammissione gratuito patrocinio, oltre a quelli afferenti alla reperibilità ed alla corrispondenza con gli stessi, di natura bancaria e postale;
- dati comuni di terzi, forniti dai clienti per l'espletamento degli inca-

richi affidati allo studio e necessari per l'espletamento di ogni tipo di attività di tutela giudiziaria, compresi i dati sul patrimonio e sulla situazione economica, necessari per fini fiscali, oltre a quelli afferenti alla reperibilità ed alla corrispondenza con gli stessi, di natura bancaria e postale;

- dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali e dati di natura bancaria e postale;
- dati comuni di altri professionisti ai quali lo studio affida incarichi e si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, inerenti a finalità fiscali, di natura bancaria e postale;
- dati sensibili e giudiziari del personale dipendente, conseguenti al rapporto di lavoro, e inerenti i rapporti con gli enti previdenziali ed assistenziali;
- dati giudiziari dei clienti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, e idonei a rivelare la qualità di imputato e indagato;
- dati giudiziari di terzi idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, e idonei a rivelare la qualità di imputato e indagato;
- dati sensibili dei clienti, dagli stessi forniti o comunque acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare l'origine razziale ed etnica, le convinzioni e l'adesione ad organizzazioni a carattere religioso, politico, sindacale e filosofico, lo stato di salute e la vita sessuale;
- dati sensibili di terzi, forniti dai clienti o comunque acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute o la vita sessuale.

R 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.

Registro delle attività di trattamento
(art. 30 c. 1 e 2 Regolamento UE 2016/679 - GDPR)

DATI DEL TITOLARE DEL TRATTAMENTO
Nome e cognome _____
Data e luogo di nascita _____
P.IVA/C.F. _____
Indirizzo dello Studio _____
N. telefono _____
Email _____
PEC _____

DATI DEL RESPONSABILE DEL TRATTAMENTO (EVENTUALE)
Nome e cognome _____
Data e luogo di nascita _____
P.IVA/C.F. _____
Indirizzo dello Studio _____
N. telefono _____
Email _____
PEC _____

Responsabile della Protezione dei Dati (DPO) (SE PREVISTO DALLA LEGGE)
Nome e cognome _____
Data e luogo di nascita _____
P.IVA/C.F. _____
N. telefono _____
Email _____
PEC _____

Data di creazione: _____
Aggiornamenti: _____

REGISTRO DEI TRATTAMENTI

Tipo di Studio e aree di specializzazione	Denominazione del trattamento (se individuata)	Finalità del trattamento	Software, Database, Manutenzione, Misure adottate	Interessati	Dati personali raccolti	Categorie di destinatari a cui i dati sono o possono essere comunicati	Denominazione responsabili esterni (se presenti)	Paesi Terzi o organizzazioni internazionali verso cui i dati possono essere trasferiti e relative garanzie	Periodo di conservazione dei dati e diritto alla cancellazione
Penale/Civile/ Lavoro	Gestione clienti	Assistenza in procedimenti giudiziali/ stragiudiziali	Software X; backup Y; Manutenzione gestita da tecnico Z (contatti tecnico PC); antivirus N	Gestione e assistenza clienti	Dati relativi all'identificazione (specificare tipo di dati personali conservati - nome, indirizzo...); atti forniti dal cliente (contratti, bozze contrattuali, fotocopie fatture, documentazione medica, corrispondenza cartacea e telematica, scritture private); documenti per assistenza giudiziale e stragiudiziale (dati anagrafici, visure, certificati casellari, sentenze, citazioni a giudizio, atti di precetto, atti amministrativi)	Collaboratori; praticanti; segretaria; commercialista	Dott. X (commercialista)	(in caso di grandi Studi con sedi all'estero)	X anni (specificare se vi sono regole particolari - es. obbligo di conservare fascicoli per almeno X anni, documenti fiscali da conservare per almeno 10 anni...)
	Gestione del personale	Gestione rapporto di collaborazione	Software X; backup Y; Manutenzione gestita da tecnico Z (contatti tecnico PC); antivirus N	Dipendenti e collaboratori (interni o esterni), praticanti	Dati identificativi; dati bancari	Commercialista; consulente del lavoro	Dott. X (commercialista); Dott. Y (consulente del lavoro)		X anni

Base giuridica su cui si fonda il trattamento - art. 6 GDPR	Tipologia di trattamento	Base giuridica del trattamento	Consenso degli Interessati	Modalità di conservazione dei dati	Azioni richieste per la conformità al GDPR	Diritto di accesso ai dati personali
Mandato difensivo conferito in data X	Trattazione legata al rapporto contrattuale, anche da parte di collaboratori e/o praticanti	Obbligo legale	Implicito nel mandato conferito (base di liceità ex art. 6 - trattamento necessario all'esecuzione di un contratto di cui l'interessato è parte)	Fascicoli cartacei/ cartelle su server	Identificare le azioni che rendono il trattamento conforme a GDPR (es. cancellazione dati non più utili)	Identificare una procedura per la gestione delle richieste di accesso ai dati da parte dell'interessato
Rapporto professionale iniziato in data X		Esercizio di un dovere	Derivante da rapporto lavorativo (base di liceità ex art. 6: - trattamento necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento)	Digitale		

Misure organizzative adottate per la prevenzione dei rischi	Misure tecniche adottate per la prevenzione dei rischi
Nomina degli incaricati - aggiornamento periodico delle caratteristiche dell'ambito del trattamento consentito ai medesimi	Antivirus X
Accessi in Studio controllati: elenco dei soggetti autorizzati all'ingresso	Procedura di identificazione informatica e aggiornamento password
Archivio chiuso a chiave - collocazione dei fascicoli idonea	Aggiornamenti software periodici
Formazione dei dipendenti	Backup periodico archivi informatici
Adesione a codici di condotta (specificare tipo)	

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.

Si illustra brevemente l'analisi dei rischi che può essere fatta in uno Studio Legale. Per i dati comuni del personale dipendente, dei clienti, di terzi, dei fornitori, degli altri professionisti cui lo studio affida incarichi, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione può definirsi medio/basso. Per i dati sensibili e giudiziari del personale dipendente, dei clienti, di terzi, dagli stessi forniti o comunque acquisiti: il rischio legato alla loro gestione è da definirsi medio/basso, poiché il trattamento avviene esclusivamente all'interno dei locali dello studio.

Per esempio il rischio di accesso all'interno dello studio da parte di soggetti non autorizzati può essere definito basso, atteso che l'ingresso nell'orario di apertura è controllato da personale dipendente o da incaricati. Il rischio di accesso all'interno delle singole stanze dello studio può essere definito basso, atteso che l'ingresso di terzi estranei avviene solo previa accettazione e controllo. Il rischio di accesso alle singole postazioni di lavoro da parte di persone non autorizzate può essere definito basso, poiché è controllato l'accesso di terzi allo studio e la zona di attesa è distanziata dalle singole postazioni di lavoro e controllabile dalla segreteria.

Avendo adottato le disposizioni di sicurezza stabilite dal D.lgs. 81/2008 ed essendo presente il dispositivo "salvavita", il rischio elettrico e di incendi conseguenti può comunque definirsi basso.

Non può tuttavia escludersi che le aree ed i locali potrebbero essere interessati da eventi imprevedibili, quali incendi, allagamenti e corto circuiti, o possa verificarsi la possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici).

Per quanto riguarda gli strumenti elettronici, il rischio di accesso ai dati in essi contenuti può essere definito basso, essendo state adottate le misure di sicurezza volte a ridurre il rischio di perdita e di accesso non autorizzato dei dati.

Non sono consentite duplicazioni di dati per finalità differenti da quelle stabilite per il trattamento.

Per quanto riguarda la documentazione cartacea, il rischio può essere definito basso, essendo gli archivi chiusi a chiave e gli armadi dotati di serrature ed essendo state adottate le altre misure indicate, fatta eccezione ovviamente per gli eventi imprevedibili.

Per quanto concerne i documenti ricevuti a mezzo fax il rischio di accesso non autorizzato alle informazioni in essi contenute è medio - basso, ciò in considerazione del posizionamento della macchina telefax posta in zona protetta da intrusioni di personale non autorizzato.

Per quanto riguarda i supporti di memorizzazione, il rischio di deterioramento dei dati in essi contenuti può essere ritenuto basso, attesi i frequenti back up, ed il fatto che essi sono conservati in armadi dotati di serrature, così come i supporti di installazione dei programmi software adottati, quando lasciati dai fornitori in disponibilità.

Gli elaboratori presenti all'interno dello studio non sono tra loro connessi in rete e risultando ciascuno accessibile unicamente mediante digitazione di password personale, il loro impiego è possibile unicamente da parte dell'utilizzatore della singola postazione di lavoro.

Atteso – infine – che gli incaricati al trattamento dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione dello Studio o di persone che con esso hanno stretti contatti, può essere definito basso.

Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori e disfunzioni da virus, in relazione ai quali sono state applicate da parte dell'incaricato della gestione del sistema informativo opportune ed idonee contromisure, più avanti meglio specificate.

Infine, si dà atto che lo studio non utilizza processi automatizzati, essendo sempre previsto l'intervento umano, ai sensi dell'art. 22 GDPR.

R 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 AVVOCATI BRESCIA

OPEN Dot Com

Il ***Gruppo Dot Com*** dal 1999 fornisce un'ampia gamma di strumenti on-line e software ad alto contenuto tecnologico, utili nello svolgimento delle professioni ordinistiche, in particolare quelle di Avvocato e di Commercialista, curandone direttamente l'assistenza attraverso Gruppi di Studio.

Grazie ad uno specifico accordo con l'Ordine, OPEN distribuisce agli Avvocati iscritti:

Consolle Avvocato®

Il software per il Processo Civile Telematico: abilitazione al Punto di Accesso, depositi telematici, consultazione di atti e provvedimenti, pagamenti telematici e gestione delle notifiche in proprio a mezzo PEC.

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.
Codice da utilizzare per usufruire dei prezzi promozionali: GDPRBS

Novità

ParcellaAvvocato

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

Per ulteriori dettagli si rimanda a:

https://www.opendotcom.it/

https://www.facebook.com/opendotcomspa

https://www.facebook.com/consolle.avvocato/