ORDINE DEGLI
AVVOCATI DI MILANO

VADEMECUM PER GLI AVVOCATI
COME GESTIRE LA PRIVACY

QUADERNI DELL'ORDINE N. 8 / MILANO 2018

☑ Presentazione

La *privacy* ha fatto irruzione nella nostra vita quotidiana e in tutti i nostri rapporti professionali e personali con una intensità imprevedibile. Esisteva infatti un codice della *privacy* del 2003, che conteneva tutte le disposizioni raccomandabili per la protezione dei dati, e su quello si erano misurate e confrontate tutte le condotte possibili, sicché il rispetto della normativa non aveva suscitato particolari disagi, né aveva determinato specifici cambiamenti. Oggi, invece, improvvisamente ci accorgiamo che una nuova regolamentazione è intervenuta (il Regolamento europeo 679/2016, direttamente applicabile agli Stati membri a far tempo della data di entrata in vigore dello stesso, il 25 maggio 2018), e questo Regolamento (che ci abitueremo a conoscere attraverso l'acronimo GDPR, General Data Protection Regulation), ha cambiato la prospettiva per le numerose disposizioni introdotte e gli altrettanti numerosi specifici adempimenti previsti.

Il Regolamento infatti non indica più le misure minime da attuare, ma impone anche all'avvocato la responsabilità (*accountability*) di definire le misure più adeguate tra tutte quelle possibili, e di garantire poi la conformità al Regolamento (*compliance*) dei trattamenti eseguiti, e tutto ciò con lo scopo di assicurare la protezione delle persone fisiche nel trattamento dei dati, specialmente di quelli sensibili.

Protezione in questo caso equivale a *privacy*, che è il rispetto etico dovuto verso gli altri, ed è un sentimento incombente, che agisce di per sé, per il solo fatto che esista un rapporto tra soggetti, e ancor più quando per l'utilizzazione dei dati sia necessario un espresso consenso. È un territorio senza limiti che impone doveri di vigilanza, controllo, informazione e protezione nei confronti di una serie innumerevole di soggetti, con i quali si costituisce un rapporto (i dipendenti, gli iscritti agli albi, i praticanti iscritti ai registri, i fornitori, i giudici, gli incolpati dei procedimenti disciplinari, i candidati agli esami di avvocato, e così via).

Nell'ambito di questa enorme platea, devono essere eseguite una serie di attività e così, ad esempio, dopo la necessaria mappatura dei rischi con la relativa valutazione, deve essere introdotto il registro dei

trattamenti; devono essere svolte attività di sorveglianza, controllo e verifica, e ancora di formazione e informazione; devono essere nominati un responsabile e un DPO (*Data Protection Officer*), nei casi previsti e deve essere assicurato sempre e comunque il rispetto dei princìpi che regolano la materia, ben noti ai cultori delle norme etiche: la liceità e la correttezza, la trasparenza, la buona amministrazione, l'accuratezza, l'integrità e la confidenzialità, insieme con altri princìpi particolari quali il principio di finalità, di necessità e minimizzazione e di limitazione all'archiviazione.

Poi vi è il soggetto passivo esposto al trattamento, chiamato *data subject*, ed egli pure ha una serie notevole di diritti: il diritto di accesso soprattutto e poi il diritto alla rettifica, all'oblio, alla limitazione del trattamento, alla opposizione, a far valere la portabilità dei dati e a ricevere le informazioni urgenti e immediate, e le notifiche relative, in caso di violazione dei suoi diritti, anche da parte di terzi.

Né va dimenticato un più alto livello di protezione riconosciuto sul piano internazionale: il "rispetto della vita privata e familiare" affermato dall'articolo 8 della Convenzione europea dei diritti dell'Uomo, per il quale la protezione dei dati personali è un diritto assoluto, fondamentale della persona. Da quell'articolo (che opera nei rapporti tra privati e pubbliche autorità) è derivata, sempre nell'ambito del Consiglio d'Europa, la più specifica Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, la n. 108 del 1981, alla quale aderiscono ben 51 paesi, non soltanto europei, e che si applica anche ai rapporti tra privati. Convenzione appena aggiornata da un Protocollo addizionale, in linea con lo sviluppo tecnologico e in sintonia con il Regolamento europeo, che sarà firmato il 25 giugno 2018 dall'Assemblea Parlamentare del Consiglio d'Europa.

In gran parte del mondo, dunque, il diritto all'informazione e alla trasparenza, e così il diritto di imprese, enti e professionisti ad utilizzare i dati anche per finalità di mercato, dovrà essere bilanciato con il prevalente diritto alla protezione dei dati personali, alla conoscenza dell'utilizzo che ne sarà fatto e alla facoltà di manifestare o rifiutare il proprio assenso, salvo le limitazioni e gli obblighi posti dalla legge.

È necessario approfondire tutto questo e ampliare le conoscenze su piattaforme che non pensavamo dovessero essere oggetto di così ferrea argomentazione, quando poi una regolamentazione ispirata da obiettivi difformi e anche divergenti (quella ad esempio che riguarda l'Autorità garante della concorrenza del mercato, ove tutto sembra lecito per accrescere la competizione) apre e chiude prospettive diverse e contrarie.

Dovremo dunque tener conto di questo grande sistema, destinato non soltanto a regolamentare la normalità, ma anche a sconfiggere la sua violazione. Pensiamo agli esempi più recenti con l'appropriazione, la divulgazione e lo sfruttamento di milioni di dati personali riservati; pensiamo al modello negativo che è ormai comportamento consolidato nel *cyber-bullismo* dei giovani studenti delle nostre scuole; pensiamo al furto di identità o di immagine, di cui si segnalano i primi casi anche nella professione. Dovremmo dunque cominciare a individuare e combattere gli abusi e credere nella necessità di assestare le regole di compatibilità per il rispetto delle persone.

Questa è la prospettiva nel tempo dei *big data* e dei *social media*, che ci impone di riflettere sui cambiamenti in essere; e quando poi le macchine, e gli algoritmi e le intelligenze artificiali che le governano prenderanno il sopravvento, dovremo pensare che il futuro si è fatto presente e nuove imprevedibili sfide dovranno essere affrontate. È dunque di almeno momentaneo conforto pensare che le difficoltà odierne sono senz'altro più facilmente superabili di quelle che ci aspettano nel prossimo futuro. Per renderle ancora più comprensibili e superabili, l'Ordine di Milano ha realizzato questo Quaderno che contiene obiettivi e indicazioni soprattutto di carattere pratico: un vero e proprio vademecum curato da un esperto della materia come l'avvocato Alice Pisapia, e completato in appendice dalla guida redatta dal Consiglio Nazionale Forense.

Il Presidente
del Consiglio dell'Ordine degli Avvocati di Milano
Remo Danovi

25 maggio 2018

INDICE

Vademecum per gli avvocati. Come gestire la privacy

1. Introduzione 5
2. Novità normative nel panorama europeo 6
3. L'avvocato e la Privacy 7
4. L'Ordine degli Avvocati di Milano e la Privacy 12
5. Qualche definizione 14
6. I principi 15
7. L'acquisizione del consenso 18
8. Cosa deve fare l'avvocato per adeguarsi al Regolamento europeo sulla privacy? 19
9. Registri delle attività di trattamento 22
10. Sanzioni 28

Appendice - Il GDPR e l'Avvocato
a cura della Commissione CNF in materia di Privacy 29

VADEMECUM PER GLI AVVOCATI
COME GESTIRE LA PRIVACY

☑ 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 per-

sonali 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 Ufficia-

le 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.

☑ 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.

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 nonché 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).

☑ 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 al 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 al regolamento per l'opinamento e il rilascio del parere di congruità dei compensi relativi ad attività professionale forense. Ai sensi del pre-

sente 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 di Milano, 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 di Milano 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 (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.

☑ 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.

☑ 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 per adeguarsi al 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 siste-

mi 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 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, 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.

☑ 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 Assessment

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.

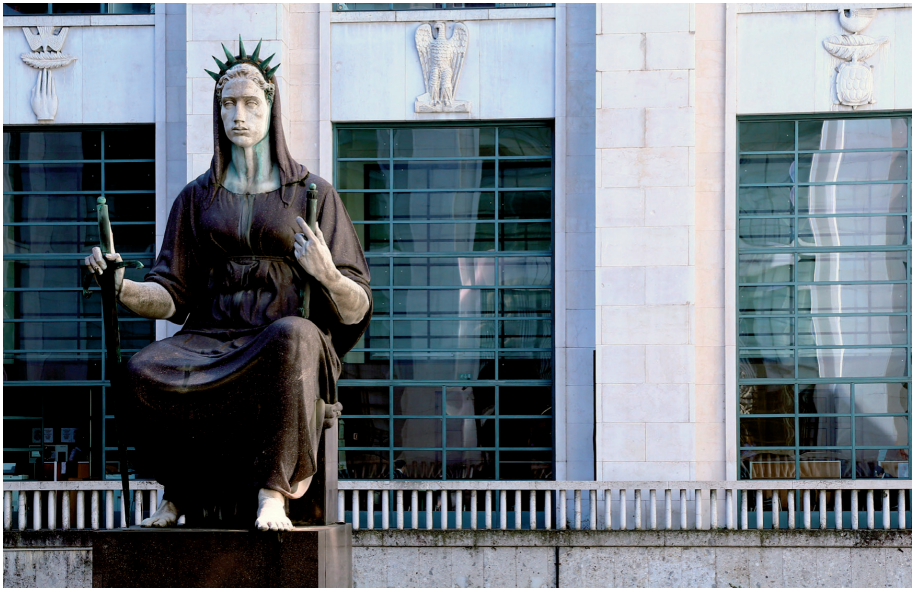
Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori e disfunzioni da virus, in relazione ai quali sono state applicate da parte dell'incaricato della gestione del sistema informativo opportune ed idonee contromisure, più avanti meglio specificate.

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

☑ 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.



Appendice

IL GDPR E L'AVVOCATO

a cura della Commissione CNF in materia di Privacy

La presente appendice fa parte del Quaderno n. 8, collana dell'Ordine degli avvocati di Milano destinata gratuitamente agli iscritti e pubblicata non a scopi commerciali. Si ringrazia il Consiglio nazionale forense per averne gentilmente concesso l'utilizzo. Il testo costituisce un adattamento grafico della Guida predisposta dal CNF, rilasciata con licenza Creative Common "CC BY-NC".

INDICE

Introduzione 33

UNO SGUARDO DI INSIEME 35
I PRINCIPI DEL GDPR 35
ACCOUNTABILITY (RESPONSABILIZZAZIONE) 36
MINIMIZZAZIONE DEI DATI 37
DIRITTO ALLA CANCELLAZIONE - DIRITTO ALL'OBLIO 38
LA VALUTAZIONE DI IMPATTO 39
LA PORTABILITÀ DEI DATI 40
L'INFORMATIVA SUL TRATTAMENTO DEI DATI 41
• Contenuto dell'informativa 43
• Come va resa l'informativa 44
CONSERVAZIONE DEI DATI 45
IL CONSENSO 46
IL DIRITTO DI ACCESSO AI DATI 47
PRIVACY BY DEFAULT E PRIVACY BY DESIGN 48

SCHEDE PRATICHE 49

1. L'AVVOCATO QUALE TITOLARE
DEL TRATTAMENTO DEI DATI 50
Quando l'avvocato è titolare? 50
In uno studio associato chi è il titolare? 51
L'avvocato domiciliatario è titolare? 51
L'avvocato deve tenere un registro dei trattamenti? 52
Quali dati tratta l'avvocato? 53
a. I dati relativi ai dipendenti e ai collaboratori 53
L'avvocato può effettuare controlli sull'attività
dei dipendenti / collaboratori? 54

Per quanto tempo devono essere conservati i dati relativi al personale dipendente ed ai collaboratori? 54
L'avvocato deve dare informativa ai dipendenti e collaboratori in merito al trattamento dei dati? 54
Riassumendo 55

b. I dati relativi al cliente 56
Quali dati tratta l'avvocato nell'ambito del suo rapporto con il cliente? 56
Dati particolari 56
Dati relativi a condanne penali e reati 56
L'avvocato deve seguire formalità particolari nel trattamento dei dati del cliente? 57
È necessario fornire una informativa al cliente? 57
Per quanto tempo devono essere conservati i dati del cliente? 58
Cosa deve fare l'avvocato in caso di revoca del mandato? . . . 58
La sicurezza del fascicolo 59
Riassumendo 59

2. IL RAPPORTO CON I SOGGETTI ESTERNI ALLO STUDIO . . . 60
La figura del responsabile del trattamento 60
Chi è il responsabile del trattamento? 60
Cosa fare nel caso in cui vi sia un responsabile del trattamento dei dati 60
Come opera il responsabile del trattamento? 62
Cosa fare con i responsabili del trattamento con i quali lo studio ha già relazioni commerciali 62
Quando l'avvocato è responsabile del trattamento? 62
Riassumendo 63

3. IL SITO WEB DELLO STUDIO 64
Cosa deve fare l'avvocato in caso di raccolta di dati attraverso il sito internet? 64

Contenuti del sito 65
Contenuti obbligatori previsti dal codice deontologico 65
Contenuti obbligatori previsti dall'art. 7 D. Lgs. n. 70/2003 (attuazione della direttiva 2000/31/CE sul commercio elettronico) a pena di una sanzione amministrativa da € 103 a € 10.000 . . 65
Contenuti obbligatori previsti dal GDPR. 65
Come rendere l'informativa nel sito in caso di utilizzazione di cookies 65
Riassumendo 66

4. L'ADOZIONE DI BUONE PRASSI PER LA SICUREZZA DEI DATI 67
Quali misure adottare? 67
In caso di documenti o fascicoli analogici 67
In caso i documenti o fascicoli gestiti digitalmente 67
Riassumendo 68

5. IL RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO 69
Lo studio legale deve nominare un DPO?. 69
Quali sono i compiti del DPO? 71
L'avvocato come DPO 71

6. DATA BREACH 72
RIASSUMENDO. 75

7. LE SANZIONI. 76

☑ Introduzione

Il Regolamento UE 2016/679 relativo alla protezione dei dati personali sarà direttamente applicabile negli Stati membri a partire dal 25 maggio 2018.

Anche gli studi legali, indipendentemente dalla loro dimensione, dalla struttura e dall'area di attività dovranno adeguarsi.

I dati ai quali l'avvocato nell'esercizio delle sue funzioni ha accesso sono, per loro natura, particolarmente sensibili: essi possono infatti riguardare la salute, l'orientamento religioso politico o sessuale, dati giudiziari, situazione familiare, dati di minori etc, ed il loro trattamento obbedisce ad una logica specifica, diversa da quella dell'impresa commerciale, essendo intimamente connessa al rapporto di fiducia che lega l'avvocato al suo cliente e al rispetto degli obblighi deontologici, primo fra tutti l'obbligo di garantire il segreto professionale.

La divulgazione, anche accidentale di tali dati potrebbe ledere i diritti e la libertà delle persone coinvolte: l'avvocato dovrà pertanto avere una cura particolare nel proteggere tali dati, conformandosi alle previsioni normative che regolano la materia.

La protezione dei dati personali del cliente, oltre ad essere essenziale per garantire il segreto professionale, rappresenta un fattore di trasparenza e confidenzialità nel rapporto.

Al fine di evitare i pericoli della perdita di tali dati, gli avvocati dovranno prestare particolare attenzione a che:

- Le finalità di trattamento dei dati e la loro trasmissione siano chiaramente definite;
- Le misure di sicurezza (tanto informatica che fisica) siano precisamente individuate, definite e attuate;
- Le persone coinvolte (segreteria, praticanti, colleghi, collaboratori a qualsiasi titolo) siano adeguatamente informate e coinvolte nel processo di protezione dei dati personali.

L'avvocato dovrà anche tenere presente che il progresso tecnologico deve comunque rispettare gli obblighi deontologici e normativi: pertanto, anche nelle ipotesi in cui lo studio abbia esternalizzato a terzi alcuni servizi (ad esempio l'utilizzo di una segreteria virtuale, la

conservazione dei dati su cloud), o utilizzi propri mezzi di comunicazione a terzi (sito web, blog, servizi di consultazione on line, utilizzo di siti terzi), dovrà prestare la massima attenzione a che i dati siano trattati in modo sicuro e nel rispetto delle norme.

Il nuovo Regolamento, oltre ad individuare i principi cui ci si deve attenere ai fini della protezione dei dati del cliente, consente all'avvocato nuovi spazi di intervento professionale: quali giuristi in possesso di particolari competenze potranno infatti prestare consulenza in materia di privacy ai loro clienti, e rivestire le funzioni di responsabile della protezione dei dati, ove in possesso anche di competenze tecniche specifiche.

La presente guida vuole essere un aiuto agli avvocati per consentire loro di adeguarsi alla normativa in materia di protezione dei dati personali.

Non pretende di essere esaustiva, anche in considerazione sia del fatto che il Regolamento, con l'introduzione del principio di responsabilizzazione (accountability) prevede che ciascuno conformi le misure da adottare alla propria organizzazione, sia che, al momento della sua redazione, non è ancora stato approvato in via definitiva il decreto legislativo di adeguamento e armonizzazione dell'ordinamento al GDPR (decreto che, pur non incidendo sull'applicabilità diretta delle norme del Regolamento, dovrebbe introdurre regole specifiche in tema di trattamenti di alcune categorie particolari di dati, nonché dei dati giudiziari, e prevedere delle specifiche norme transitorie), e sarà pertanto soggetto a modifiche ed ampliamenti.

Roma,li 22 maggio 2018

La commissione privacy
Carla Secchieri (coordinatrice)
Nicola Fabiano (componente esterno)
Giovanni Battista Gallus (componente esterno)
Francesco Paolo Micozzi (componente esterno)
Alessio Pellegrino (segretario)

Un particolare ringraziamento ai componenti del Gruppo di Lavoro della FIIF.

UNO SGUARDO DI INSIEME

☑ I PRINCIPI DEL GDPR

Il regolamento riafferma principi fondamentali già in vigore con la precedente legislazione e ne aggiunge di nuovi. Tra i principi relativi al trattamento dei dati che vengono confermati:

- **finalità del trattamento:** che ne limita l'utilizzo ai soli fini degli obiettivi di tutela, consulenza e difesa perseguiti con specifico mandato dell'avvocato (titolare del trattamento); ad esempio i dati raccolti nelle visure catastali non possono essere utilizzati per conoscere la vita privata degli assistiti, e neppure utilizzati a scopi commerciali, di pubblicità politica o elettorale;
- **necessità e proporzionalità:** il trattamento deve essere adeguato, pertinente e necessario allo scopo; ad esempio non appare opportuno estendere una raccolta di informazioni e dati relativi all'entourage familiare, se sono necessari solo alcuni dati inerenti l'attività professionale; i fascicoli delle pratiche e l'archiviazione informatica degli stessi devono essere configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali ed identificativi;
- **durata limitata:** il trattamento non può protrarsi oltre il tempo necessario per l'espletamento degli incarichi, ovvero oltre il tempo necessario in funzione del mandato e della finalità del trattamento stesso compresi gli obblighi legali di conservazione; nell'informativa all'assistito è essenziale indicare la ragionevole durata del trattamento stesso (considerando che nel concetto di trattamento rientra anche la mera conservazione del fascicolo contenente dati personali, a prescindere dal fatto che si tratti di fascicolo informatico o cartaceo);
- **sicurezza e riservatezza:** l'avvocato è tenuto, anche per obblighi deontologici e, nel rispetto del segreto professionale, ad approntare un adeguato livello di sicurezza per i dati degli assistiti. L'avvocato, pertanto, nella sua qualità di titolare del trattamento deve prevedere tutte le misure necessarie per garantire la confidenzia-

lità, integrità e disponibilità dei dati personali: i dati contenuti nel fascicolo, ad esempio, non possono essere consultati da persone non abilitate ed espressamente istruite e autorizzate ad accedervi in ragione dei loro specifici compiti, sia che si tratti di soggetti interni all'organizzazione dello studio legale (addetti alla segreteria, praticanti, colleghi di studio) o esterni allo stesso (co-difensori, consulenti tecnici, commercialisti etc).

- rispetto del diritto delle persone.

Sono poi stati introdotti ulteriori principi e doveri cui l'avvocato deve uniformarsi:

- Il principio di accountability, alla quale si è già fatto cenno (o principio di responsabilizzazione);
- La minimizzazione dei dati;
- Il diritto all'oblio;
- il diritto alla portabilità dei dati;
- La notificazione dei data breach al Garante e, in talune ipotesi, agli interessati.

☑ ACCOUNTABILITY (RESPONSABILIZZAZIONE)

Pietra miliare di una visione differente di approccio al dato dell'interessato - ancorché riprenda quanto già previsto dall'art. 6 comma 2 della Direttiva 95/46/CE - il GDPR impone (anche) all'avvocato un profondo cambiamento culturale nel trattamento delle informazioni di cui viene in possesso o ha accesso in virtù del suo mandato e, pertanto, nella qualità di titolare del trattamento.

Rispetto al Codice Privacy, non sono più previste le c.d. misure minime, ma è posta in capo al titolare del trattamento, la responsabilità (*accountability*) di definire, dopo una attenta analisi dei dati trattati e dei possibili rischi connessi, le misure adeguate al fine di garantire il rispetto delle norme del GDPR. Responsabilizzazione significa, sostanzialmente, che le misure dovranno essere adeguate alla struttura del singolo titolare ed elaborate, caso per caso, ricorrendo ad una pre-

ventiva mappatura dei dati trattati, della mole degli stessi, dei rischi di trattamento dei dati gestiti.

Accountability, inoltre, significa qualcosa di più: significa anche essere in grado di "rendere conto" delle attività poste in essere e del fatto di aver rispettato i principi del GDPR (e ciò in base a quanto previsto dal secondo comma dell'art. 5 del GDPR). L'avvocato, pertanto, deve garantire la conformità (*compliance*, in inglese) al Regolamento dei trattamenti eseguiti (sia dal titolare che dai soggetti da lui eventualmente nominati come responsabili). Ciò significa, ad esempio, che anche l'adozione di criteri e procedure di trattamento certe e di una formazione adeguata allo studio, potrà precostituire una prova della conformità del trattamento al fine di evitare pesanti sanzioni.

☑ MINIMIZZAZIONE DEI DATI

È il principio secondo il quale i dati personali da trattare per ogni singola attività debbano essere soltanto quelli necessari per il raggiungimento dello scopo.

Consiste, ad esempio:

- nell'interrogarsi sulla necessità di trattare dati personali per raggiungere le finalità richieste dal trattamento;
- nel limitare al minimo il ricorso al trattamento dei dati personali, ove sia necessario, per quanto attiene: le categorie di dati trattati, il volume e la quantità di dati e il sapere se sono o meno necessari al trattamento.

Al fine di conformarsi al principio di minimizzazione, l'avvocato dovrà trattare, per quanto possibile, solo i dati essenziali, necessari e pertinenti per compiere la prestazione richiesta dal cliente.

Ad esempio i dati raccolti nelle visure catastali per un'indagine relativa al tenore di vita di una parte per la determinazione di congruità di un assegno di mantenimento, non possono essere utilizzati per conoscere la vita privata delle persone, e neppure utilizzati a scopi commerciali di pubblicità politica o elettorale; o ancora, non è necessario il trattamento dei dati di tutto l'entourage familiare, se sono necessari

solamente alcuni dati attinenti alla sua vita professionale (salvi gli obblighi di identificazione ed adeguata verifica imposti dalla legislazione antiriciclaggio).

☑ DIRITTO ALLA CANCELLAZIONE - DIRITTO ALL'OBLIO

L'art. 17 del GDPR (C65, C66) prevede il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano ed il correlativo obbligo di adempiere senza ingiustificato ritardo da parte del titolare stesso. Il diritto all'oblio, si era di recente affermato per impulso della giurisprudenza a seguito della celebre Sentenza della Corte di Giustizia Europea, Grande Sezione, C-131/12 del 13 maggio 2014 (c.d. Google Spain) Esso si sostanzia, ad esempio, nel diritto del singolo non già alla radicale eliminazione dell'informazione ma alla non rinvenibilità della stessa, ovvero, nel mondo web, alla deindicizzazione delle informazioni personali dai motori di ricerca così che non fossero facilmente rintracciabili.

Rispetto a tale assetto previgente, il GDPR si spinge oltre, richiedendo una vera e propria eliminazione del dato, e non la sua mera deindicizzazione: è necessario, in altri termini, che i dati vengano completamente soppressi dall'archivio del titolare. Tale diritto, così esattamente correlato con i principi di proporzionalità, durata limitata e minimizzazione del trattamento, presuppone che venga effettuato un controllo di proporzionalità tra gli interessi della persona interessata e quelle del titolare del trattamento o, se del caso, del pubblico in generale (diritto all'informazione o interesse storico). L'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o sia venuto meno il motivo per cui sono stati forniti.

Per l'avvocato il diritto all'oblio non potrà essere esercitato sino quando non sia maturato il termine di prescrizione dell'azione per la responsabilità professionale. È importante rilevare, inoltre, che l'esercizio del diritto in parola cede il passo di fronte all'adempimento di alcuni obblighi di archiviazione dei dati per periodi specifici e risulta pertanto non utilmente esercitabile ove comprometta l'adempimento ad obblighi fiscali o si ponga in contrasto necessità archivistiche di pubblico interesse ovvero, infine, ove il mantenimento del dato sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

☑ LA VALUTAZIONE DI IMPATTO

L'art. 35 del GDPR (C84, C89-C93, C95) prescrive - quando sia probabile che un tipo di trattamento possa creare un elevato rischio per i diritti e le libertà delle persone fisiche, ivi compreso il trattamento su larga scala di dati particolari - che il titolare del trattamento debba effettuare una preliminare valutazione d'impatto (DPIA).

Con specifico riferimento alla figura dell'avvocato ed al trattamento dei dati dei relativi ai propri assistiti, il C91 precisa che tale trattamento non dovrebbe mai essere considerato su larga scala. Ad onta di ciò, tuttavia, la valutazione di impatto è comunque necessaria laddove vengano soddisfatti almeno due dei nove dei criteri indicati dal WP29 (valutazione-punteggio, decisione automatica con effetto legale o simili; monitoraggio sistematico; raccolta di dati sensibili; collezione dati personali su larga scala; riferimenti incrociati di dati; persone vulnerabili; uso innovativo; esclusione del beneficio di un diritto-contratto). Maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.

Per quanto possano essere considerate un onere aggiuntivo, le valutazioni d'impatto consentono ai titolari ed ai responsabili del trattamento di identificare e trattare rischi che non sarebbero stati altrimenti rilevati e per prevenire violazioni che diversamente si sarebbero verificate. Consentono all'avvocato di prendere coscienza di trattare dati personali e sensibili del cliente, e di prevedere per essi l'adozione di misure di sicurezza adeguate.

Per meglio comprendere la portata dell'art. 35, il WP 29 ha adottato delle linee guida sulla DPIA e sui trattamenti che possono causare rischi:

http://194.242.234.211/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati

Per facilitare l'esecuzione della valutazione di impatto, il Garante per la protezione dei dati personali ha messo a disposizione un software, scaricabile al seguente link:

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8581268

☑ LA PORTABILITÀ DEI DATI

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

L'art. 20 del GDPR attribuisce all'interessato il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso o su un contratto e b) il trattamento sia effettuato con mezzi automatizzati.

Ciò significa che l'avvocato che tratti i dati dei clienti *con mezzi automatizzati* (per esempio, adottando un gestionale informatico o anche solo tenendo uno schedario sotto forma di foglio di calcolo)

è tenuto a comunicare i dati del suo cliente al collega alle seguenti condizioni:

- il cliente ha espresso il suo consenso al trattamento dei suoi dati personali o il trattamento è necessario per l'esecuzione di un contratto a cui il il cliente è parte o l'esecuzione delle misure precontrattuali adottate a richiesta del cliente;
- e il trattamento è stato effettuato con mezzi automatizzati.

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

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

Secondo il WG29 il diritto alla portabilità si applica solo se il trattamento è effettuato con l'aiuto di procedure automatizzate, e pertanto non è esteso ai fascicoli cartacei, che sembrano dunque esclusi dal diritto alla portabilità.

Deve però essere ricordato che, secondo l'art. 2235 c.c., l'avvocato non ha diritto a trattenere i dati se non il tempo necessario alla tutela dei propri diritti.

I titolari del trattamento devono essere in grado di seguire e identificare i destinatari dei dati personali che elaborano, e nei casi previsti debbono tenere un registro dei trattamenti.

☑ L'INFORMATIVA SUL TRATTAMENTO DEI DATI

L'art. 13, paragrafo 1, del GDPR (C60-C62) impone all'avvocato che acquisisce i dati degli assistiti di fornire le seguenti informazioni:

1. l'identità e i dati di contatto del titolare dello studio e, ove applicabile, del suo rappresentante all'estero;
2. i dati di contatto del responsabile della protezione dei dati (ove applicabile);

3. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
4. le categorie di dati personali in questione;
5. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
6. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
   In aggiunta a tali informazioni, una volta che i dati personali siano stati acquisiti, il titolare del trattamento dovrà fornire all'interessato ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente, vale a dire:
7. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
8. l'esistenza del diritto dell'interessato di 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;
9. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
10. il diritto di proporre reclamo a un'autorità di controllo;
11. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
12. l'esistenza di un processo decisionale automatizzato, compresa la

profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'art. 14 enumera poi le informazioni da comunicare nell'ipotesi in cui i dati non siano stati ottenuti presso l'interessato: la persona deve essere informata degli elementi previsti dall'art. 13, ma allo stesso modo anche di quali dati personali, e le modalità con le quali sono state raccolte. Per gli avvocati il par. 5 dell'art. 14 prevede un'esenzione in virtù della necessità di preservare il segreto professionale: così è ad esempio il caso in cui il cliente trasmette informazioni e dati della controparte.

Gli avvocati che agiscono quali titolari dei dati sono liberi di determinare i mezzi occorrenti per assicurare l'informativa alle persone.

Tutte le persone hanno diritto di opporsi al trattamento dei dati per motivi legittimi, a meno che il trattamento non presenti un carattere obbligatorio.

In altri termini, e volendo semplificare ai minimi termini, l'avvocato è tenuto a rendere le informazioni sul trattamento dei dati esclusivamente ai propri clienti, oltre che a tutti gli altri soggetti i cui dati vengano trattati per ragioni contrattuali (fornitori, collaboratori, consulenti, con esclusione dei dati che il titolare detenga ai fini dell'adempimento di un obbligo di legge - per esempio, quanto ai dati detenuti per ragioni fiscali - così potendosi argomentare dalla lettura del considerando n. 62), ma giammai anche alle controparti.

Contenuto dell'informativa.

Alla luce dell'art. 13 del Regolamento, gli interessati al trattamento da parte di uno studio legale dovranno essere informati su:

- L'identità e i dettagli di contatto del titolare del trattamento (l'avvocato o l'associazione professionale);
- i dettagli di contatto del responsabile o dei responsabili della pro-

tezione dei dati, qualora nominati;
- Le finalità del trattamento
- La base giuridica del trattamento (prestazione contrattuale o pre-contrattuale su richiesta del cliente);
- interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. comma 1 lettera f;
- destinatari di dati (subappaltatori, ufficiali giudiziari, ecc.);
- flussi transfrontalieri;
- la durata di conservazione;
- i diritti che gli interessati possono esercitare;
- le condizioni e le modalità per l'esercizio dei diritti degli interessati;
- il diritto di revocare il consenso, se questo è la base giuridica del trattamento;
- il diritto di presentare un reclamo all'autorità di controllo;
- le informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.

Come va resa l'informativa.

Alla luce del considerando n. 58 e dei chiarimenti resi al riguardo dal Garante, l'informativa deve avere forma concisa, trasparente, comprensibile per l'interessato e facilmente accessibile. Essa dev'essere scritta in un linguaggio chiaro e semplice ma può essere resa anche in formato elettronico (ad esempio, se destinate al pubblico, attraverso un sito web) o comunicata via e-mail (ad esempio, in occasione della trasmissione di una nota di onorario in particolare per regolarizzare la situazione con i clienti che non sono stati adeguatamente informati). Quanto ai minori, considerato che meritano una protezione specifica, il regolamento dispone che, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.

Con specifico riferimento alla professione forense, l'informativa può essere data anche nel corpo dell'accordo contrattuale

Sono ammesse icone per la sua composizione, purché queste siano accompagnate da una informativa estesa (queste icone dovranno

essere uguali in tutta Europa e saranno definite dalla Commissione Europea).

Il testo dell'informativa può anche essere inserito nel sito web dell'avvocato, a condizione che poi l'avvocato possa dimostrare che l'informativa è stata letta, ad esempio inserendo nel testo della procura che il cliente ha preso visione dell'informativa pubblicata sul sito, e di averla ben compresa.

Si ricorda, peraltro, che per il considerando n. 62, l'informativa sul trattamento non è dovuta "...(a) se l'interessato dispone già dell'informazione, (b) se la registrazione o la comunicazione dei dati personali sono previste per legge (c) o se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato." (come nel caso dei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici).

☑ CONSERVAZIONE DEI DATI

L'avvocato titolare del trattamento deve definire una politica di durata e di conservazione dei dati nel suo ufficio. I dati personali possono essere conservati solo per il tempo necessario per il completamento dell'obiettivo perseguito durante la loro raccolta.

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

È inoltre importante ricordare che i dati acquisiti in sede di identificazione e adeguata verificata ai sensi del decreto legislativo n. 231 del 2007 in materia di antiriciclaggio devono essere conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della

prestazione professionale o dall'esecuzione dell'operazione occasionale (art. 31, comma 3, d. lgs. 231 del 2007).

☑ IL CONSENSO

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

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

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Quantunque non sia richiesto un consenso scritto, e sebbene l'attività professionale possa rientrare nella lettera b), è preferibile precostituirsi la prova di avere ottenuto il consenso (art. 7, par. 1, del GDPR): l'avvocato, quindi, dovrà sottoporre al cliente per la firma una dichiarazione di consenso in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive (C42). È facoltà dell'interessato revocare il proprio consenso in qualsiasi momento (art. 7, par. 2, del GDPR), ma "*la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca*".

☑ IL DIRITTO DI ACCESSO AI DATI

Il GDPR apporta le rilevanti modifiche anche sul diritto di accesso.

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

- per sapere se sta trattando i suoi dati;
- per ottenere la comunicazione dei dati in forma comprensibile e tutte le informazioni disponibili per quanto attiene l'origine del trattamento;
- per ottenere informazioni sulla finalità del trattamento i dati raccolti e i destinatari.

Sinteticamente:

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

Commissioni di riproduzione: il regolamento prevede un principio di gratuità copie fornite come parte di una richiesta di accesso (art. 12.5). Questo solo quando la domanda è manifestamente infondata o eccessiva che il il responsabile del trattamento può richiedere il pagamento di "costi ragionevoli" che tengono conto dei costi amministrativi sostenuti per la fornitura delle informazioni. La medesima regola si applica quando viene richiesta una copia aggiuntiva dei dati.

Le modalità di comunicazione dei dati: il regolamento prevede che se la persona inoltra una domanda per via elettronica, l'informazione richiesta è comunicata in forma elettronica di uso comune, a meno che l'interessato non richieda diversamente (art. 12.3).

Prevede inoltre che il responsabile del trattamento assista il titolare nell'adempimento dei suoi obblighi riguardo al diritto di accesso (art. 28 e). Ad esempio: un datore di lavoro potrebbe chiedere al proprio responsabile del trattamento di fornirgli supporto per fornire ai dipendenti che lo richiedono geolocalizzazioni "in forma accessibile".

☑ PRIVACY BY DEFAULT E PRIVACY BY DESIGN

L'art. 25 del GDPR prevede l'obbligo di integrare di default il concetto di dati personali nella progettazione di nuovi prodotti e servizi. Quando l'avvocato cambia i suoi software, pertanto, si deve interrogare sin dall'inizio in merito all'impatto dell'evoluzione sui dati che tratta. Ciò implica in particolare l'integrazione di tecniche di protezione e misure organizzative per limitare i rischi di violazione dei diritti e delle libertà delle persone.

SCHEDE PRATICHE

☑ 1 - L'AVVOCATO QUALE TITOLARE DEL TRATTAMENTO DEI DATI

Quando l'avvocato è titolare?

Ai sensi dell'art 4 comma 7 GDPR (C74) il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Il termine inglese "Data Controller" ben si concilia con il carattere gestionale di colui che può determinare finalità e mezzi del trattamento.

L'avvocato sarà titolare del trattamento di tutte le informazioni che vengono allo stesso fornite dagli assistiti in virtù o in correlazione del mandato ricevuto.

Il GDPR prevede altresì (art. 26, C79) la figura dei contitolari del trattamento quando più titolari determinano congiuntamente le finalità e i mezzi del trattamento. Si reputa che nel mondo forense questa figura possa ravvisarsi in tutti i casi in cui vi sia un mandato a più colleghi che lavorano insieme ed in collaborazione determinando insieme le finalità e le modalità del trattamento. In questi casi è necessario un esplicito accordo interno che definisca le rispettive responsabilità ed osservanza degli obblighi, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR.

Nel caso in cui, invero, ciascun avvocato riceva mandato per specifiche prestazioni o attività, pur inerenti lo stesso oggetto di controversia, consulenza o problematica, non si ravvisa una collaborazione nelle finalità e, pertanto, ciascuno sarà autonomo titolare del trattamento elaborando autonomamente le modalità di trattamento. È il caso, ad esempio, di assistenza specifica di più avvocati ciascuno in ambiti diversi ed autonomi, come - anche all'interno dello stesso studio - l'avvocato cui è affidata la difesa in sede civile e l'avvocato cui è affidata la difesa in sede penale da parte del medesimo soggetto per fatti correlati.

In uno studio associato chi è il titolare?

Nel caso di società o associazioni è sempre l'ente giuridico - in nome del legale rappresentante - ad essere qualificato titolare; ciononostante, in virtù del mandato tra assistito e avvocato, mandato di natura prettamente personale e fiduciaria, si reputa che il titolare non potrà che ravvisarsi nell'avvocato che riceve (o negli avvocati della società o associazione che ricevono) incarico della prestazione e non nel legale rappresentante della persona giuridica. Nel caso, infatti, in cui il fiduciario cessi i propri rapporti professionali con l'associazione o la società, l'incarico fiduciario con quel professionista è autonomo, e la società o associazione non dovrebbe più reputarsi titolata a detenere la totalità delle informazioni fornite. Nella pratica non potrebbe avocare un diritto di titolarità delle informazioni del fascicolo o di tutti i dati relativi al singolo assistito, ma, per applicazione dei criteri di necessità, proporzionalità e minimizzazione dei soli dati pertinenti e necessari, come ad esempio, a fini fiscali.

L'avvocato domiciliatario è titolare?

Si reputa che l'avvocato mero domiciliatario, poiché tratta dati personali per conto del dominus mandatario (titolare del trattamento), sia da qualificarsi Responsabile ai sensi dell'art. 4 par. 8 del GDPR.

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

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

L'avvocato deve tenere un registro dei trattamenti?

Il registro delle attività di trattamento elenca le informazioni sulle caratteristiche dei trattamenti effettuati dal titolare del trattamento.

Ogni titolare del trattamento di dati dovrà tenere un registro delle categorie di trattamento dei dati personali implementati sotto la sua responsabilità. Tale obbligo non vige per le organizzazioni con meno di 250 dipendenti, a meno che il trattamento non includa un rischio per i diritti e le libertà delle persone interessate, non occasionale o se si riferisce in particolare a dati sensibili o a dati relativi a condanne e reati.

Uno studio legale sarà quindi soggetto all'obbligo di istituire un registro delle attività trattamento allorché il trattamento sia riferito a particolari categorie di dati o dati relativi a condanne e reati sanzioni (esemplificativamente: gli avvocati che si occupano di diritto penale, quelli che si occupano di famiglia e minori, di diritto della previdenza sociale, di *medical malpractice* e, in generale, di vertenze in materia di risarcimento danni da lesioni personali).

In ogni caso la detenzione del registro è fortemente consigliata anche all'avvocato che - ipotesi quasi di scuola - tratti soltanto dati comuni, consentendogli di mappare più chiaramente i trattamenti e di monitorare gli stessi ai fini del rispetto dei principi del GDPR e dei diritti degli interessati, oltre a risultare molto utile, ove occorra, per fornire prova dell'esatto adempimento all'obbligo adeguamento al principio dell'*accountability*.

Tale registro, in conformità con l'articolo 30 del GDPR, deve includere le seguenti informazioni:

- Il nome e i dettagli di contatto del titolare, del contitolare, del responsabile e, se del caso, il rappresentante del responsabile della elaborazione e responsabile della protezione dei dati;
- gli scopi del trattamento;
- Una descrizione delle categorie di dati trattati, nonché delle categorie di persone coinvolte nel trattamento;
- Categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari dei paesi parti terze o organizzazioni internazionali;
- Ove applicabile, i trasferimenti di dati personali verso un paese terza parte o un'organizzazione internazionale, compresa l'identi-

ficazione di paese terzo o di tale organizzazione internazionale e i documenti che certificano l'esistenza di garanzie adeguate;
- ove possibile il termine ultimo previsto per la cancellazione dei dati;
- ove possibile una descrizione generale delle misure di sicurezza tecniche ed organizzative.

Quali dati tratta l'avvocato?

L'avvocato tratta:
- i dati relativi al personale dipendente ed ai collaboratori;
- i dati relativi ai clienti;
- i dati raccolti attraverso il sito internet.

a. I dati relativi ai dipendenti e ai collaboratori

Nell'ambito dei rapporti di collaborazione o di lavoro (ad esempio con una segretaria o il tecnico del computer) della gestione del libro paga e la gestione amministrativa del personale, l'avvocato – in qualità di datore di lavoro effettua un trattamento di dati. Lo deve pertanto effettuare in conformità alle norme del GDPR, ricordando che l'art. 88 prevede discrezionalità degli stati membri nella regolamentazione del trattamento dei dati nell'ambito del rapporto di lavoro (ad oggi il decreto legislativo non è ancora stato emanato).

Nel contesto della gestione dei suoi dipendenti e, più in generale, il suo personale, l'avvocato come il datore di lavoro può raccogliere principalmente due tipi di dati:
- Dati necessari per ottemperare a un obbligo legale.
- Dati utili per:
  (i) gestione amministrativa del personale,
  (ii) organizzazione lavoro e
  (iii) azione sociale.

Durante il colloquio per l'assunzione, i dati dovrebbero essere usati solo per valutare la capacità del candidato di eseguire il lavoro proposto.

Potranno pertanto essere raccolti solo i dati relativi alla qualifica e all'esperienza del collaboratore (esempi: diplomi, precedenti lavori, ecc.).

È pertanto vietato:
- raccogliere dati sulla famiglia del candidato;
- raccogliere dati su opinioni politiche o appartenenza sindacale il candidato.

L'avvocato può effettuare controlli sull'attività dei dipendenti / collaboratori?

L'avvocato del datore di lavoro può utilizzare strumenti per controllare l'attività dei dipendenti o del personale.

Ad esempio, lo studio legale potrebbe determinare le condizioni di utilizzo dell'accesso a Internet da parte di dipendenti e personale sul luogo di lavoro: può inserire i filtri per bloccare determinati contenuti (pornografia, pedofilia, ecc.).

È anche possibile limitare l'uso di Internet per motivi di sicurezza, ad esempio il download di software, o predisporre strumenti atti a controllare le ore di lavoro o l'accesso da parte dei dipendenti ai files.

Non è invece possibile estendere al controllo dell'attività dei dipendenti l'utilizzo di un eventuale software installato al fine di calcolare il tempo dedicato dall'avvocato allo studio o alla predisposizione di atti di un fascicolo.

Per quanto tempo devono essere conservati i dati relativi al personale dipendente ed ai collaboratori?

In base al principio generale per cui il trattamento non può protrarsi oltre il tempo necessario per l'espletamento degli incarichi, ovvero il tempo necessario in funzione della finalità del trattamento stesso, i dati relativi ai dipendenti o ai collaboratori potranno essere conservati per il tempo della durata del rapporto, aumentato dell'eventuale tempo di maturazione della prescrizione, al fine di far valere i diritti nascenti dal rapporto.

L'avvocato deve dare un'informativa ai dipendenti e collaboratori in merito al trattamento dei dati?

In conformità con i requisiti dell'art. 13 del GDPR, i dipendenti e i collaboratori dello studio legale dovrebbero essere informati in merito a:

- L'identità e i dettagli di contatto del titolare del trattamento;
- I dettagli di contatto del responsabile della protezione dei dati quando ce n'è uno;
- L'obiettivo perseguito (gestione amministrativa del personale e assunzioni);

- la base legale del trattamento;
- interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. comma 1 lettera f;
- Destinatari dei dati (chi tiene i libri paga, ecc.);
- flussi transfrontalieri;
- la durata di conservazione;
- Condizioni di esercizio dei loro diritti di opposizione, accesso, rettifica e limitazione, ecc.;
- Il diritto di revocare il consenso se è la base giuridica del trattamento;
- Il diritto di presentare un reclamo all'autorità di controllo;
- Informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.

Questa informazione può essere inserita nell'accordo di collaborazione o nel contratto di lavoro, ovvero può essere oggetto di documento visualizzato o può essere inviata comunicazione via e-mail, in particolare per regolarizzare la situazione con dipendenti e personale che non sono stati adeguatamente informati.

RIASSUMENDO

COSA DEVE FARE L'AVVOCATO?
1. VERIFICARE CHE I DATI RACCOLTI NON SIANO ECCESSIVI RISPETTO ALLA FINALITA' DEL TRATTAMENTO
2. VERIFICARE CHE CI SIA UNA BASE LEGALE PER IL TRATTAMENTO DEI DATI
3. RISPETTARE IL PRINCIPIO DI MINIMIZZAZIONE
4. VERIFICARE I DISPOSITIVI DI CONTROLLO DELL'ATTIVITA' DEL PERSONALE E LA LORO PERTINENZA
5. INSERIRE I DATI NEL REGISTRO DI TRATTAMENTO DEI DATI (ove tenuto)
6. DEFINIRE LA DURATA DI CONSERVAZIONE DEI DATI
7. DARE L'INFORMATIVA AGLI INTERESSATI

b. *I dati relativi al cliente*

Quali dati tratta l'avvocato nell'ambito del suo rapporto con il cliente?

Dati particolari

Nell'ambito dell'esercizio della professione di avvocato, il trattamento dei dati personali del cliente riguarda tutti i dati necessari per la formazione del fascicolo del cliente e per la difesa dei suoi interessi.

Data la diversità dei campi di intervento degli avvocati, questi dati possono essere molto diversi e possono essere relativi alla vita personale, ma anche i dati di che rivestono una particolare sensibilità: l'avvocato infatti potrebbe avere a che fare con dati personali che rivelano l'origine razziale o opinioni etniche, politiche, credenze religiose o filosofiche, l'appartenenza sindacale, così come l'elaborazione di dati genetici, dati biometrici ai fini dell'individuazione di una persona fisica, dati sanitari unici o di vita, orientamento sessuale.

L' articolo 9, comma 1 del GDPR prevede il divieto in linea di principio del trattamento di tali dati.

Tuttavia, l'articolo 9 prevede un'eccezione al comma 2 f) per "*accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionale*".

Gli avvocati possono quindi trattare dati particolari nell'esercizio della professione purché i dati in questione siano strettamente necessari per esercitare o difendere i diritti dei clienti.

Ovviamente è raccomandata una interpretazione rigorosa di questa necessità, anche nel rispetto del principio di minimizzazione di cui si è detto più sopra.

Dati relativi a condanne penali e reati

L'avvocato al fine di poter espletare il proprio incarico può/deve raccogliere dati sulle condanne penali e sui precedenti del cliente. La natura speciale di questi dati richiede garanzie di un trattamento specifico.

L' articolo 10 del GDPR prevede che tale trattamento possa essere

effettuato solo sotto il controllo dell'autorità pubblica, o regolamentato da disposizioni specifiche previste dalla legge nazionale.

L'avvocato deve seguire formalità particolari nel trattamento dei dati del cliente?

Laddove il trattamento di dati particolari sia effettuato dall'avvocato in modo non occasionale è opportuno che sia previsto nel registro dei trattamenti un apposito modulo relativo ai dati del cliente, che deve includere i seguenti elementi:

- Identità e dettagli di contatto del titolare del trattamento;
- scopi;
- Categorie di persone interessate;
- Categorie di dati personali;
- Categorie di destinatari;
- Trasferimenti verso un paese terzo o un'organizzazione internazionale;
- Termine finale del trattamento;
- Descrizione generale delle misure di sicurezza tecniche e organizzative.

È necessario fornire una informativa al cliente?

In conformità con i requisiti della sezione 13 del GDPR, i clienti di uno studio legale dovrebbero essere informati su:

- L'identità e i dettagli di contatto del titolare del trattamento (la ditta);
- i dettagli di contatto del responsabile della protezione dei dati quando ce n'è uno;
- L'obiettivo perseguito (gestione e monitoraggio dei file dei clienti);
- La base giuridica del trattamento (prestazione contrattuale o precontrattuale su richiesta del cliente);
- interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. comma 1 lettera f;
- destinatari di dati (subappaltatori, ufficiali giudiziari, ecc.);
- flussi transfrontalieri;
- la durata di conservazione;

- i diritti che hanno;
- Condizioni per l'esercizio di questi diritti;
- Il diritto di revocare il consenso se è la base giuridica del trattamento;
- Il diritto di presentare un reclamo all'autorità di controllo;
- Informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.

Queste informazioni possono essere incluse nell'accordo con il cliente; possono anche essere comunicate via e-mail o in occasione della trasmissione di una nota di onorario, in particolare per regolarizzare la situazione con i clienti che non sono stati adeguatamente informati.

Per quanto tempo devono essere conservati i dati del cliente?

L'avvocato titolare del trattamento deve definire una politica di durata e di conservazione dei dati nel suo ufficio. I dati personali possono essere conservati solo per il tempo necessario per il completamento dell'obiettivo perseguito durante la loro raccolta. In generale, i dati dei clienti possono essere tenuti per la durata del mandato professionale.

I dati dovranno essere conservati inoltre, prima della loro cancellazione definitiva sino a che un'eventuale azione di responsabilità professionale in cui potrebbe essere implicato l'avvocato, non sia prescritta.

Cosa deve fare l'avvocato in caso di revoca del mandato?

Come già rilevato più sopra con riferimento al diritto di portabilità dei dati, l'avvocato che ha inizialmente trattato i dati è tenuto a comunicare i dati del suo cliente o di un collega alle seguenti condizioni:

- il cliente ha espresso il suo consenso al trattamento dei suoi dati personali o il trattamento è necessario per l'esecuzione di un contratto a cui il il cliente è parte o l'esecuzione delle misure precontrattuali adottate a richiesta del cliente;
- il trattamento è stato effettuato con mezzi automatizzati.

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

Si rammenta che ove il fascicolo fosse tenuto in modalità esclusivamente cartacea, non si applica il diritto alla portabilità, ma il fascicolo deve essere consegnato al cliente nel minor tempo possibile, con l'eccezione delle lettere riservate che dovranno essere consegnate direttamente all'avvocato che lo ha sostituito.

La sicurezza del fascicolo

È necessario adottare misure di sicurezza adeguate alla sensibilità dei trattamenti.

L'avvocato è inoltre soggetto al segreto professionale assoluto e deve, ancor più per questo motivo, assicurare la sicurezza dei dati affidatigli dai suoi clienti.

Per fare ciò, è necessario verificare che l'accesso ai locali in cui sono conservati o memorizzati i fascicoli sia sufficientemente sicuro (uffici bloccati, accesso badge, ecc.). È anche importante verificare la sicurezza del sistema informatico su quali file sono memorizzati in formato digitale (firewall, password robuste per accesso, diritti, ecc.).

RIASSUMENDO

COSA DEVE FARE L'AVVOCATO?
1. VERIFICARE CHE I DATI RACCOLTI NON SIANO ECCESSIVI RISPETTO ALLA FINALITA' DEL TRATTAMENTO
2. VERIFICARE CHE CI SIA UNA BASE LEGALE PER IL TRATTAMENTO DEI DATI
3. RISPETTARE IL PRINCIPIO DI MINIMIZZAZIONE
4. DEFINIRE LA DURATA DI CONSERVAZIONE DEI DATI
5. INSERIRE I DATI NEL REGISTRO DI TRATTAMENTO DEI DATI (ove tenuto)
6. VERIFICARE CHE I FASCICOLI DEI CLIENTI TANTO DIGITALI CHE CARTACEI SIANO CONSERVATI IN MODO SICURO
7. VERIFICARE LA SICUREZZA DEL SISTEMA INFORMATICO CON IL FORNITORE IT

☑ 2 - IL RAPPORTO CON I SOGGETTI ESTERNI ALLO STUDIO

La figura del responsabile del trattamento

Chi è il responsabile del trattamento?

Ai sensi dell'art. 4, par. 8 il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che "tratta dati personali **per conto** del titolare del trattamento".

È importante sottolineare il concetto del trattamento dei dati personali "per conto" del titolare del trattamento. Il responsabile, in sostanza, effettua il trattamento in quanto i dati personali gli sono comunicati dal titolare del trattamento.

In pratica, è la persona che tratta dati personali per conto dello studio legale come un contabile, un editore di software, un host web, ecc.

Il responsabile è da considerarsi solo "esterno" allo studio legale; pertanto non è possibile nominare un Collega, un dipendente o un collaboratore come responsabile della protezione dei dati. I soggetti a cui lo studio comunica i dati personali trattati sono considerati responsabili del trattamento (es.: commercialista, consulente del lavoro, consulente, fornitori di servizi digitali, conservatori di documenti informatici, ecc.).

Nella ipotesi in cui vi sia un responsabile del trattamento (un soggetto esterno) e qualora fosse una persona fisica, la prima cosa da fare è fornire l'informativa al momento della raccolta dei suoi dati personali. Nel caso di persone giuridiche si può procedere con la sottoscrizione del contratto così come illustrato nel paragrafo seguente.

Cosa fare in caso in cui vi sia un responsabile del trattamento dei dati

L'art. 28, comma 3, del GDPR prevede l'obbligo di stipulare un contratto tra titolare e responsabile del trattamento, dettagliando i suoi contorni e stabilendo requisiti rigorosi sugli aspetti severi e più importanti.

Il contratto dovrà includere:

- l'oggetto;
- la durata;
- natura;
- lo scopo;
- il tipo di dati personali;
- le categorie di persone interessate;
- i diritti e gli obblighi del responsabile del trattamento;
- le misure di sicurezza attuate in relazione al trattamento dei dati che sarà effettuato.

Il contratto deve anche definire gli **obblighi** del responsabile relativi a:

- la possibilità di elaborare dati solo su un'istruzione documentata del titolare del trattamento anche per quanto riguarda i flussi transfrontalieri;
- riservatezza dei dati;
- l'esercizio dei diritti delle persone interessate;
- l'assistenza che deve essere fornita al titolare tramite con misure tecniche e organizzative adeguate, nella misura in cui sia possibile, per consentire al titolare di adempiere all'obbligo di rispondere alle richieste delle persone interessate;
- l'assistenza fornita al titolare per assicurare il rispetto dei suoi obblighi in relazione alla natura del trattamento e delle informazioni a disposizione del responsabile;
- la cancellazione dei dati in questione alla fine del trattamento, o la loro restituzione al titolare o alla loro conservazione se richiesto da a disposizione nazionale o europea;
- la messa a disposizione del titolare dei dati tutte le informazioni necessarie a dimostrare la conformità agli obblighi e a consentire condurre verifiche, comprese le ispezioni, da parte del titolare o di suo incaricato, e collabora in questi audit;
- l'eventuale assunzione da parte del responsabile di altro responsabile per l'esecuzione di specifiche attività di trattamento per conto del titolare. L'incarico che deve essere formalizzato in un contratto che preveda tutti gli obblighi sopra elencati.

Le clausole contrattuali che vincolano i titolari e responsabili devono pertanto essere molto precise sia sulle modalità di trattamento che sulla gestione delle loro relazioni e sullo scambio di informazioni tra di loro.

Ai sensi dell'articolo 28, paragrafo 1, del GDPR il responsabile del trattamento dei dati ha l'obbligo di incaricare solo responsabili "che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".

Il GDPR stabilisce (art. 28, par. 2, GDPR) che il responsabile può nominare a sua volta un responsabile (subresponsabile) ma tale nomina è subordinata a esplicita autorizzazione scritta del titolare del trattamento.

Come opera il responsabile del trattamento ?

Ai sensi dell'art. 29 del GDPR "Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri". Pertanto, sono esplicitamente richieste istruzioni specifiche al responsabile del trattamento da parte del titolare; tali istruzioni potranno essere indicate nel contratto tra il titolare e il responsabile.

Cosa fare con i responsabili del trattamento con i quali lo studio ha già relazioni commerciali

Gli studi legali dovranno interpellare i loro subappaltatori sulle garanzie adottate per garantire la loro conformità con il GDPR.

Nel caso in cui lo studio legale identifichi lacune nelle misure adottate dal responsabile dovranno integrare il contratto al fine di colmarle.

Quando l'avvocato è responsabile del trattamento?

L'Avvocato può anche essere responsabile del trattamento dei dati personali nel momento in cui - ad esempio - gli venga richiesta una

consulenza da un soggetto che è titolare del trattamento. Allo stesso modo, l'avvocato può essere responsabile del trattamento allorquando riceva una domiciliazione da parte di un Collega. Anche in questo caso, l'Avvocato sarà nominato responsabile del trattamento e dovrà sottoscrivere un contratto con il Collega titolare del trattamento.

Diversa è la situazione dell'Avvocato al quale viene conferita la procura congiuntamente e/o disgiuntamente ad altro Collega. In questo caso si è di fronte ad un'ipotesi di contitolarità, così come disciplinata dall'art. 26 del GDPR.

RIASSUMENDO

COSA DEVE FARE L'AVVOCATO?
1. IDENTIFICARE I RESPONSABILI DEL TRATTAMENTO
2. VERIFICARE LA CONFORMITA' DEI RESPONSABILI E LE MISURE ADOTTATE NEL CONTRATTO STIPULATO CON IL RESPONSABILE
3. MODIFICARE, OVE NECESSARIO IL CONTRATTO GIA' ESISTENTE

☑ 3 - IL SITO WEB DELLO STUDIO

Gli avvocati possono utilizzare siti web per promuovere la loro attività, presentare i componenti dello studio, o pubblicare articoli ma il sito web può anche consentire la raccolta di dati personali con diverse modalità:

- un questionario online;
- una consultazione online;
- un modulo di contatto;
- creazione di un account online;
- attraverso i cookies.

La titolarità di un sito web comporta principalmente la pubblicazione di una informativa, redatta ai sensi degli articoli 13 e 14 del GDPR.

Cosa deve fare l'avvocato in caso di raccolta di dati attraverso il sito internet?

Qualora il sito web dello studio permetta l'inserimento di dati personali (es. modulo di contatto), è opportuno che sia utilizzata la connessione con protocollo sicuro HTTPS (tecnologia "SSL") per garantire il rispetto delle misure di sicurezza in funzione della confidenzialità delle informazioni scambiate con il professionista.

L'avvocato dovrà inserire, all'interno del registro delle attività di trattamento, un apposito modulo dedicato al trattamento dei dati sul sito web che deve includere i seguenti elementi:

- Identità e dettagli di contatto del titolare;
- scopi;
- Categorie di persone;
- Categorie di dati personali;
- Categorie di destinatari;
- trasferimenti verso un paese terzo o un'organizzazione internazionale;
- Scadenze per la cancellazione;
- Descrizione generale delle misure di sicurezza tecniche e organizzative.

Qualora l'avvocato riceva una proposta di incarico tramite il sito web sussiste l'obbligo di formalizzare il mandato accertando l'identità del cliente (art. 23 cod. deont.).

Contenuti del sito

Contenuti obbligatori previsti dal codice deontologico

- Indicazione del titolo professionale, la denominazione dello studio e l'ordine di appartenenza (art. 35, c. 3, cod. deont.);
- Il praticante può utilizzare soltanto il titolo per esteso "praticante avvocato" con l'eventuale indicazione di "abilitato al patrocinio" qualora abbia conseguito l'abilitazione (art. 35, c. 5, cod. deont.).

Contenuti obbligatori previsti dall'art. 7 D. Lgs. n. 70/2003 (attuazione della direttiva 2000/31/CE sul commercio elettronico) a pena di una sanzione amministrativa da euro 103 ad euro 10.000

- riferimento alle norme professionali e al codice deontologico e le modalità di consultazione dei medesimi;
- il numero della partita IVA.

La L. n. 247/2012 esclude i compensi tra le informazioni che possono essere diffuse.

Contenuti obbligatori previsti dal GDPR

- Obbligo ai titolari di siti web di informare gli utenti che visitano il sito sulle modalità di utilizzo dei cookie;
- Informativa sul trattamento dei dati;
- le informazioni di cui agli artt.13 e 14.

Come rendere l'informativa nel sito in caso di utilizzazione dei cookies

Come prima cosa, gli avvocati dovranno verificare l'effettiva presenza di cookie sul loro sito web attraverso il dipartimento IT dell'azienda, i fornitori di servizi o controllando gli strumenti utilizzati, ecc.

Successivamente, è necessario determinare i tipi di cookie utilizzati sul sito web dell'avvocato. In effetti, alcuni cookie richiedono il con-

senso dell'utente, questo è il caso per:

- cookie pubblicitari;
- cookie "social network" generati dai pulsanti di condivisione quando raccolgono dati personali senza il consenso delle persone interessate;
- alcuni cookie di misurazione degli accessi.

In questo caso, il consenso deve essere precedente all'inserimento o alla lettura del contenuto del sito. Finché il cliente non ha dato il suo consenso, questi cookie non possono essere depositati o letti dal sito stesso.

RIASSUMENDO

COSA DEVE FARE L'AVVOCATO?
1. INTEGRARE I CONTENUTI LEGALI OBBLIGATORI DEL SITO ☐
2. INTEGRARE I CONTENUTI CON QUANTO PREVISTO DAL GDPR ☐
3. INSERIRE I DATI NEL REGISTRO DI TRATTAMENTO DEI DATI ☐
4. VERIFICARE LA PRESENZA DI COOKIES ☐
5. IDENTIFICARE LA TIPOLOGIA DI COOKIES ☐
6. CREARE UN BANNER DI RACCOLTA DEL CONSENSO ☐
7. INSERIRE LA MENZIONE SUI COOKIES ☐

☑ 4 - L'ADOZIONE DI BUONE PRASSI PER LA SICUREZZA DEI DATI

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

L'avvocato è soggetto al segreto professionale. Questo obbligo rafforza la necessità di misure di sicurezza negli studi legali poiché in caso di violazione dei dati personali dei clienti, è segreto professionale che viene violato. La sfida della sicurezza non è quindi banale per l'avvocato.

Quali misure adottare?

In caso di documenti o fascicoli analogici

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

- Limitare l'accesso all'ufficio;
- Non archiviare fascicoli o documenti contenenti dati personale in locali dello studio accessibili a tutti;
- Installare gli allarmi nei locali dello studio.

In caso di documenti o fascicoli gestiti digitalmente

Si consiglia di:

- Autenticare gli utenti: impostare una password minima di 8 caratteri contenenti maiuscole, lettere minuscole, numeri e caratteri speciale; non condividerla; non scriverla chiaramente su un foglio; evitare la pre-registrazione; cambiarla regolarmente;
- gestire i diritti e istruire gli utenti: determinare persone che hanno il diritto di accedere ai dati personali;
- rimuovere le autorizzazioni di accesso obsolete;
- scrivere un regolamento di utilizzo del computer e inserirlo nel regolamento interno nell'ipotesi che sia stato adottato;
- mobile computing sicuro: fornire mezzi di crittografia per computer portatili e dispositivi di archiviazione rimovibili (chiavette USB, CD, DVD ...), evitare di memorizzare dati personali sensibili dei clienti.

- eseguire il backup e pianificare la business continuity: implementare i backup regolarmente, conservare i supporti di backup in un luogo sicuro, ecc.

RIASSUMENDO

COSA DEVE FARE L'AVVOCATO?
MISURE DI SICUREZZA FISICHE
1. LIMITARE L'ACCESSO ALLO STUDIO ☐
2. VERIFICARE E METTERE IN SICUREZZA I LUOGHI OVE SONO CONSERVATI I FASCICOLI ☐
3. INSTALLARE SISTEMA DI ALLARME ☐
MISURE DI SICUREZZA DIGITALI
1. PREVEDERE MISURE DI IDENTIFICAZIONE DELL'UTILIZZATORE ☐
2. GESTIRE LE ABILITAZIONI E SENSIBILIZZARE L'UTILIZZATORE ☐
3. METTERE IN SICUREZZA I DISPOSITIVI MOBILI ☐
4. EFFETTUARE IL CENSIMENTO DEGLI ASSET (BENI FISICI O DIGITALI) UTILIZZATI NEL TRATTAMENTO DEI DATI ☐
5. EFFETTUARE LA VALUTAZIONE DEI RISCHI CONNESSI A CIASCUN ASSET E ADOTTARE LE RELATIVE CONTROMISURE ☐
6. PIANIFICARE LA BUSINESS CONTINUITY ☐
ADOTTARE UN REGOLAMENTO DI UTILIZZO DEL COMPUTER
ADOTTARE PROCEDURE DI NOTIFICAZIONE DELLE VIOLAZIONI DEI DATI PERSONALI

☑ 5 - IL RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO

Lo studio legale deve nominare un DPO?

Ai sensi dell'articolo 37 del GDPR, i titolari del trattamento e i responsabili dovranno nominare un responsabile della protezione dei dati ogniqualvolta:

- il trattamento sia effettuato da un'autorità, un organismo ovvero un ente pubblico;
- le attività principali del titolare del trattamento e del responsabile del trattamento richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
- se le loro attività principali (core business) li portano a trattare (su larga scala) categorie specifiche di dati, noti come dati "sensibili" e dati su condanne penali e reati;

Negli altri casi, la nomina di un responsabile della protezione dei dati è ovviamente possibile, come opzione organizzativa ulteriore e di maggior cautela.

I titolari del trattamento possono optare per un *responsabile per la protezione* di dati condiviso con altri, ovvero per un delegato interno all'organizzazione od esterno.

Il gruppo di lavoro articolo 29 (WP29), composto da rappresentanti delle Autorità Nazionali per la protezione dei dati degli Stati membri dell'UE, ha pubblicato linee guida sul ruolo dei responsabili della protezione dei dati e fornito raccomandazioni per adottare buone prassi.

Se viene nominato un responsabile della protezione dei dati, lo studio legale obbligato a pubblicare le informazioni relative al DPO e a farne comunicazione all'autorità di controllo competente.

Tuttavia, la previsione dell'art. 37 (così come quella dell'art 35) si applica sempre al titolare o al responsabile del trattamento di categorie dati particolari. Queste disposizioni richiedono la nomina del DPO nei casi in cui *le attività principali* della persona del titolare o del responsabile consistono in un trattamento *su larga scala* delle categorie di dati di cui all'articolo 9.

Secondo le linee guida dei responsabili della protezione dei dati, "*per attività principali*" si possono intendere le operazioni essenziali

che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare del trattamento o del responsabile del trattamento. Per esempio, il trattamento di dati relativi alla salute (come le cartelle sanitarie dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un RPD".

Va inoltre correttamente interpretata l'espressione "*larga scala*", e ciò in quanto anche un piccolo studio legale potrebbe dover affrontare trattamenti di una notevole mole di dati sensibili: al riguardo, si evidenzia che il considerando 91 del GDPR - così come le stesse esemplificazioni delle linee guida - consentono di sostenere che questo requisito non si applica agli avvocati ed in genere ai professionisti organizzati su base individuale (cfr punto 1.3.2.4 sulla valutazione dell'impatto).

Pertanto, pur potendosi ritenere che la maggior parte degli studi legali non trattino siffatti dati personali su larga scala che pertanto, la nomina di un responsabile della protezione dei dati non è richiesta, la valutazione dell'opportunità o meno di nominare un delegato alla protezione i dati deve essere effettuata caso per caso, in funzione in particolare dei seguenti parametri:

- numero di persone interessate dal trattamento di dati personali,
- volume dei dati trattati,
- la durata,
- permanenza delle attività del trattamento,
- estensione geografica dell'attività di trattamento.

Vale, in ogni caso, la medesima regola espressa per il DPIA (documento di valutazione di impatto per la protezione dei dati): per quanto non obbligatoria, la designazione di un *Data Protection Officer* potrebbe essere valutata dagli studi legali come un'opportunità organizzativa nell'ormai imprescindibile gestione dei trattamenti.

Quali sono i compiti del DPO?

Il GDPR impone ai DPO degli obblighi importanti: sono come dei direttori di orchestra della conformità in materia di protezione dei dati personali in seno all'organismo che li ha nominati, sono incaricati di:

- Informare e consigliare il titolare o il responsabile, e i loro dipendenti;
- Assicurare il rispetto del regolamento e della legge nazionale in merito alla protezione dei dati;
- Informare l'organizzazione sulla realizzazione di studi di impatto sulla protezione dati e verificarne l'esecuzione;
- Collaborare con il Garante ed esserne il punto di contatto;
- Collaborare nell'adeguamento agli obblighi imposti dal regolamento europeo, fornendo informazioni sul contenuto dei nuovi obblighi imposti dal regolamento europeo;
- Condurre un inventario del trattamento dei dati della propria organizzazione;
- Progettare azioni di sensibilizzazione;
- Gestire in maniera continuativa la conformità dell'organizzazione al regolamento.

Le responsabilità che sorgono in capo alla persona designata come DPO sono quindi rilevantissime.

L'avvocato come DPO

Si potrebbe pensare che un avvocato potrebbe essere la persona più indicata a rivestire il ruolo di DPO, ma deve essere chiaro come, avendo presenti le diversità di compiti previsti dal regolamento, una persona nominata come DPO deve avere nozioni tecniche maggiori rispetto alle semplici competenze legali.

Laddove l'avvocato dovesse svolgere funzioni di DPO dovrà tenere presente che i compiti, le funzioni e le verifiche imposti dal Regolamento UE non richiedono conoscenze di esclusiva natura legale.

Inoltre, l'assimilazione delle due funzioni (avvocato / DPO) e il rischio di confusione tra queste funzioni sono un punto da valutare con estrema attenzione da parte di qualsiasi avvocato che abbia la possibilità di essere nominato come responsabile della protezione dei dati su

richiesta di un cliente. In tali casi, l'avvocato si troverebbe ad alternarsi tra la funzione di DPO e lo svolgimento dei compiti di consulenza e difesa dei diritti tipici della professione. Egli dunque dovrà essere in grado di garantire la propria indipendenza e di evitare conflitti di interesse, che potrebbero derivare dall'essere contemporaneamente sia la persona di contatto dell'autorità di protezione dei dati (un ruolo che comporta l'obbligo di riferire all'autorità anche se è in contrasto con l'interesse del cliente) sia colui che tutela e rappresentare gli interessi dei clienti in sede giudiziaria e stragiudiziale. In considerazione di questo potenziale conflitto di interessi, sarebbe opportuno che l'avvocato assumesse il ruolo di DPO solo laddove non abbia agito come legale di fiducia in questioni che potrebbero rientrare nella responsabilità del DPO. Egli inoltre, durante il loro mandato come DPO, non dovrebbe assumere compiti di difesa in questioni in cui dovesse essere coinvolto in qualità di DPO.

☑ 6 - DATA BREACH

In virtù degli artt. 33 e 34 del GDPR uno studio di avvocato che agisce quale titolare del trattamento deve notificare tutte le violazioni dei dati personali al Garante e comunicare con le persone interessate in caso di alto rischio per i diritti e la libertà personali.

La violazione dei dati personali, il c.d. data breach, è una violazione della sicurezza che comporta accidentalmente o illecitamente, distruzione, perdita, alterazione, divulgazione o accesso non autorizzati di dati di natura personale trasmessi, conservati o altrimenti elaborati.

Il titolare del trattamento ha l'obbligo di documentare - e di esibire ad eventuale richiesta del Garante - qualsiasi violazione dei dati personali, le circostanze che l'hanno causata, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Se lo studio legale si è avvalso di un responsabile del trattamento, quest'ultimo ha l'obbligo di notificare al titolare, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza, qualsiasi violazione

dei dati personali. È raccomandabile che tale obbligo sia oggetto di una specifica clausola contrattuale con il responsabile.

In ottemperanza agli artt. 33 e 34 del GDPR uno studio legale che agisce quale titolare del trattamento, in caso di alta probabilità di rischio dei diritti e delle libertà personali, deve notificare al Garante e comunicare agli interessati tutte le violazioni dei dati personali di cui viene a conoscenza.

In applicazione del principio generale di accountability, è rimessa all'avvocato titolare del trattamento la valutazione di probabilità o meno che lo specifico data breach possa presentare un rischio per i diritti e le libertà degli assistiti e degli interessati. Laddove la valutazione abbia esito affermativo, non oltre le 72 ore dalla presa di coscienza (GDPR, art. 33) l'avvocato (titolare del trattamento) deve notificare la violazione al Garante della protezione dei dati personali (in qualità di autorità competente), specificando, tra l'altro:

- la natura della violazione dei dati personali (categorie e numero approssimativo di persone e record di dati in questione);
- Il nome e le informazioni di contatto del DPO (laddove applicabile) o, comunque, di un punto di contatto da cui è possibile ottenere ulteriori informazioni;
- le probabili conseguenze della violazione;
- le misure adottate o da adottare per mitigare qualsiasi conseguenze negative.

Si raccomanda inoltre di:

- mettere in atto misure per analizzare i rischi del trattamento istituito per i diritti e le libertà delle persone fisiche;
- assicurarsi che le violazioni siano notificate entro 72 ore, in caso contrario spiegare accuratamente le motivazioni del ritardo all'autorità garante;
- indicare nella notifica i fatti della violazione, la natura della violazione, i suoi effetti e le misure adottate per porvi rimedio;
- fare ogni sforzo per documentare il più possibile qualsiasi violazione per consentire all'autorità di vigilanza di verificare la conformità ai requisiti imposti dal GDPR;

- mettere immediatamente in atto misure di emergenza per porre rimedio alla violazione e mitigare le conseguenze.

Comunicazione alle persone interessate.

Laddove il titolare valuti che sia probabile che la violazione sia suscettibile di presentare un elevato rischio per i diritti e le libertà di una persona fisica, sarà necessario comunicare anche all'interessato il data breach. Tale comunicazione deve contenere almeno:

- le informazioni del nome e dei dati di contatto del DPO (ove applicabile) o di altro punto di contatto presso cui ottenere maggiori informazioni;
- la descrizione - con un linguaggio semplice e chiaro - della natura della violazione dei dati personali e delle probabili conseguenze, le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione all'interessato può non essere necessaria se:

- le misure tecniche e organizzative preventivamente approntate dal titolare hanno reso i dati incomprensibili per qualsiasi persona; ciò capita, ad esempio, quando tali dati, pur diffusi, sono stati cifrati o crittografati;
- sono state adottate misure per garantire che il rischio sia scongiurato e non possa più verificarsi;
- la comunicazione richieda "sforzi sproporzionati", ma in questo caso è autorizzata una comunicazione "pubblica" piuttosto che diretta sempreché la stessa possa raggiungere ed informare gli interessati con analoga efficacia della comunicazione diretta.

La comunicazione gli interessati può anche essere richiesta dall'Autorità garante se quest'ultima reputa, dopo aver esaminato la notificazione, che vi sia un alto rischio per gli interessati derivante dal data breach.

RIASSUMENDO

COSA DEVE FARE L'AVVOCATO?
1. AVVISARE SENZA INDUGIO LE PERSONE COMPETENTI
2. QUALIFICARE LA VIOLAZIONE
3. ADOTTARE LE MISURE NECESSARIE PER MINIMIZZARE LE CONSEGUENZE
4. EFFETTUARE LE NOTIFICAZIONI ALL'AUTORITÀ GARANTE, A MENO CHE NON SIA IMPROBABILE CHE SUSSISTA UN RISCHIO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE
5. SE IL RISCHIO È ELEVATO EFFETTUARE LE COMUNICAZIONI AGLI INTERESSATI
6. IN OGNI CASO ANNOTARE TUTTE LE VIOLAZIONI (ANCHE SE NON NOTIFICATE) NEL REGISTRO DELLE VIOLAZIONI

☑ 7 - LE SANZIONI

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

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

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

COLLANA DEI QUADERNI DELL'ORDINE DI MILANO

1. Giustizia senza processo? La funzione dell'Avvocatura (XXXIII Congresso nazionale forense – Rimini, 6-8 ottobre 2016)
2. I nostri primi 10 anni. L'attività del CPO dalla nascita ad oggi: obiettivi, risultati ed esperienze (2016)
3. Le 100 domande sul PCT (2016)
4. Codice deontologico e legge professionale forense (2017)
5. Vademecum per le scuole. Educazione alla legalità (2017)
6. Vademecum. Deontologia professionale nel diritto di famiglia: Ruoli, condotte, obblighi, divieti dell'avvocato (2017)
7. Il Pct a Milano. Analisi della soddisfazione degli iscritti all'Ordine degli Avvocati di Milano rispetto al Pct (2017)
8. Vademecum per gli avvocati. Come gestire la privacy (2018)

Tutti i Quaderni sono disponibili in formato digitale sul sito dell'Ordine degli Avvocati di Milano.

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.

Per ulteriori dettagli si rimanda a:
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