REGOLAMENTO UE
Il 25 maggio 2018
diviene obbligatorio il GDPR
anche per gli studi legali

GDPR e privacy negli studi legali

REGOLE DI BASE
APPLICAZIONI PRATICHE
PROFILI DEONTOLOGICI

avv. maela coccato
avv. edoardo ferraro
avv. daniele a. m. trento
avv. antonio zago

Le guide del
Movimento
Forense
Triveneto

INTRODUZIONE

Il regolamento comunitario n. 679 del 2016, entrato in vigore il 25 maggio 2016 ma con **termine per l'adeguamento fino al 25 maggio 2018**, coinvolge anche gli studi professionali ed in particolare, gli studi legali.

Il regolamento, comunemente abbreviato con l'acronimo GDPR (*General Data Protection Regulation*) si occupa della protezione dei dati personali e di tutelare la libera circolazione dei dati e prevede significative novità rispetto al Codice c.d. Privacy portato dal d.lgs. 196/2003, passando da una tutela spesso rimasta solo formale, a una **tutela sostanziale del dato**.

In tal senso il GDPR si fonda sul principio della c.d. ***Accountability*** o responsabilizzazione del titolare del dato, non imponendo prescrizioni di dettaglio, ma chiedendo nella sostanza che il dato venga tutelato e che il titolare possa dimostrare di aver attuato azioni positive per la tutela.

L'attuale assetto degli studi legali, molto diverso da quello che si presentava nel 2003 e la necessità di una tutela sostanziale dei dati (che dipende dalla struttura e dall'organizzazione dello studio oltreché dalle soluzioni tecniche adottate) rende **difficile individuare soluzioni omogenee o standard** in grado di rendere tutti egualmente *compliant.*

Ad oggi la realtà degli studi legali vede convivere: studi formati da un unico professionista; studi associati; studi che usano spazi e servizi (es. la segreteria) condivisi; studi con sede in varie regioni se non in vari stati; STP e finanche studi con soci di capitale.

Ancora, volendo esemplificare, molti studi legali hanno un sito internet "vetrina", ma alcuni prevedono anche interazioni dirette con il cliente tramite applicazioni o l'invio di *newsletters*, etc etc.

È chiaro che, quando si parla di tutela del dato, **ad ogni realtà corrisponde un diverso grado di rischio** e, conseguentemente, saranno diverse le attività da svolgere (c.d. principio della ***Compliance***).

Il presente *vademecum,* pertanto, con tutte le limitazioni derivanti da quanto sopra indicato (necessità di valutare la *compliance* sulla base degli assetti organizzativi e tecnici dello studio e dal tipo di trattamenti effettuati dallo studio) è diretto a dare delle indicazioni di massima di "buone prassi" da seguire per l'applicazione del Regolamento.

DEFINIZIONI: PROFILO OGGETTIVO

Dati personali: *"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 a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*.

Trattamento: *"qualsiasi **operazione** o insieme di operazioni [...] e applicate a dati personali o insiemi di dati personali".*

Dati "particolari"(già detti "sensibili"): ***"dati** personali che rivelino l'origine **razziale** o **etnica,** le opinioni **politiche,** le convinzioni **religiose** o filosofiche, o l'appartenenza **sindacale,** nonché trattare dati **genetici,** dati **biometrici** intesi a identificare in modo univoco una persona fisica, dati relativi alla **salute** o alla **vita sessuale** o all'**orientamento sessuale** della persona".*
Il divieto di trattamento di tali dati non opera quando *"il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali".*

Natura dei dati raccolti:

1) **Finalizzati**: raccolti e trattati per uno scopo preciso, da indicare.
2) **Accurati**: verificati e esatti, con eventuale correzione e adeguamento.
3) **Limitati**: raccolti nei limiti di quanto serve allo scopo.
4) **Riservati**: custoditi con sistemi di sicurezza.
5) **A tempo**: trattati e conservati per il tempo strettamente necessario allo scopo.

DEFINIZIONI: PROFILO SOGGETTIVO

Titolare del Trattamento: persona fisica o giuridica che determina finalità e mezzi di trattamento dei dati personali.

1) Nel caso di **libero professionista** che esercita la professione in forma non associata è la **persona fisica** in quanto tale.
2) Nel caso di **associazioni professionali o società** tra professionisti è **l'entità** nel suo complesso.
3) Nel caso di **più avvocati** non associati in mandato, si parla di **contitolari** (due o più titolari che determinano congiuntamente le finalità e i mezzi di trattamento).

Responsabile del Trattamento: persona fisica o giuridica che tratta dati personali per conto del titolare **da nominare a mezzo contratto o altro atto giuridico**.
Si tratta di **soggetti terzi rispetto lo studio** a cui vengono affidati a mezzo contratto o incarico dati personali (es. commercialista; consulenti di parte; interpreti; consulente del lavoro; amministratore di sistema; gestore *cloud* etc.) su cui il titolare mantiene **obbligo di vigilanza** e responsabilità a titolo di ***culpa in eligendo***.

Incaricato (interno) al Trattamento: soggetto **interno all'organizzazione** aziendale su cui il titolare mantiene **obbligo di vigilanza** e responsabilità a titolo di ***culpa in eligendo***.
Va **indicato nell'organigramma** dell'organizzazione.

DPO - Responsabile Protezione Dati Personali: **soggetto designato dal titolare** o dal responsabile del trattamento per assolvere a **funzioni di supporto e controllo**, **consultive**, **formative** e informative relativamente all'applicazione del Regolamento medesimo.
Il suo nominativo **va comunicato al Garante**.
La sua **nomina non** è **obbligatoria** in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale.
Resta **comunque consigliata**.

LA BASE GIURIDICA DEL TRATTAMENTO

I dati vanno trattati in virtù di una **base giuridica** (art. 6) affinché il trattamento possa considerarsi lecito.
Non è necessario ottenere **sempre il consenso** della persona di cui si trattano i dati.
Va effettuata una **valutazione in ragione della finalità** del trattamento e **della tipologia del dato** che viene trattato.

Tipologie di Basi giuridiche del trattamento:

1) Autorizzazione generale del Garante
2) Consenso del soggetto interessato
3) Necessità di esecuzione di un contratto
4) Adempimento di un obbligo legale
5) Salvaguardia di interessi vitali
6) Necessità di esecuzione di un compito o un interesse pubblico

Esemplificazioni di basi giuridiche del trattamento:

1) per i dati necessari a **far valere un diritto in giudizio** potrà trovare fondamento nel provvedimento di **autorizzazione generale** del Garante;
2) per i dati necessari a **far valere un diritto in sede stragiudiziale** potrà trovare fondamento nel contratto di **conferimento di incarico** (che stabilità anche le finalità del trattamento);
3) per i dati acquisiti a **mezzo web per** l'invio di **newsletter** dovrà essere acquisito un **consenso specifico** (e dovrà essere fornita apposita informativa);
4) per i dati acquisiti a mezzo web a mezzo di un **form «collabora con noi»** (es. cv) dovrà essere acquisito un **consenso specifico** (e dovrà essere fornita apposita informativa);
5) il sito internet dovrà rispettare la c.d. *cookie law* in relazione alle eventuali attività di profilazione e dovrà in ogni caso essere dotato di idonea informativa (è dato personale anche l'identificativo online).

IL CONSENSO

Ove necessario il **consenso** per il trattamento dei dati personali, questo dovrà essere **preceduto dalle necessarie informazioni** relativamente alla finalità ed alle modalità del trattamento dei dati.

Il **consenso** dovrà riferirsi ad un specifico trattamento e ad una specifica finalità:

1) **non** può essere **generico**
2) **non** può essere **estendibile** a vari possibili trattamenti
3) va **esclusa** ogni forma di **consenso tacito** o mediante opzioni preselezionate.

L'INFORMATIVA

L'informativa (artt. 13 e 14) per la raccolta del consenso non deve essere necessariamente scritta, ma potrà essere **anche orale.**

In ogni caso, **si raccomanda di utilizzare la forma scritta** in quanto il GDPR impone al titolare di dover eventualmente *"dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali"*.
Sarà quindi utile far anche sottoscrivere una dichiarazione in tal senso.

L'informativa va **raccolta in occasione del primo incontro**, al momento in cui viene affidato l'incarico e quando si acquisiscono i dati personali.
Qualora **non** sia stata ottenuta **presso l'interessato, va fornita entro** un termine ragionevole e comunque entro **30 giorni**.
Non è necessario fornire l'informativa:

- **se l'interessato dispone già dell'informazione**;
- **se** la registrazione o la comunicazione di dati personali sono **necessarie per legge**;
- **se** informare l'interessato si rivela **impossibile o** richiederebbe uno sforzo **sproporzionato**.

I **contenuti** che l'informativa deve avere sono i seguenti:

- **l'identità e i dati di contatto del titolare** del trattamento e, ove applicabile, **del** suo **rappresentante**;
- i **dati di contatto del responsabile della protezione** dei dati, ove applicabile;
- le **finalità del trattamento** cui sono destinati i dati personali nonché **la base giuridica** del trattamento; qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli **eventuali destinatari** o le eventuali categorie di destinatari dei dati personali;

ove applicabile, **l'intenzione del titolare del trattamento di trasferire dati personali a 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 appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;

- **il periodo di conservazione dei dati** personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- 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**;
- l'esistenza del **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il **diritto di proporre reclamo** al Garante della Privacy o avanti al Giudice Ordinario;
- 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;
- **l'esistenza di un processo decisionale automatizzato**.

ATTENZIONE!!! Il consenso raccolto prima del 25 maggio 2018 resta valido se ha tutti i requisiti indicati nel **GDPR.** In caso contrario andrà inviata una nuova informativa per informare dei nuovi diritti del GDPR.

LE MISURE A PROTEZIONE DEI DATI PERSONALI: PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Il GDPR (art. 25) introduce i due concetti di:

1) ***privacy by design*****:** la tutela della privacy come elemento atto a prevenire il danno e non a rimediare ai problemi, nell'ottica di una tutela sostanziale e non meramente formale dei dati, caratterizzata da funzionalità e trasparenza.
2) ***Privacy by default*****:** per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

Tutto ciò è, come già detto, **responsabilità (*accountability*) del titolare del trattamento**.

Possono esemplificarsi alcune **misure** comuni che rispettino i suddetti princìpi:

- definire **procedure interne** prima di porre in essere nuovi trattamenti;
- introdurre ***policy*** **vincolanti** da applicare ai nuovi trattamenti;
- mappare i processi e gestire l'inventario (**registro attività di trattamento**);
- designare un **DPO** se necessario, o funzioni similari;
- attuare programmi di **formazione,** istruzione, sensibilizzazione **del personale**;
- definire **procedure per la gestione** dei diritti dell'interessato;
- istituire un **meccanismo interno** per la gestione dei **reclami**;
- definire **procedure** interne **per** la **notifica** delle **violazioni** della sicurezza (***data breach***);
- effettuare la **valutazione d'impatto** per i trattamenti di dati che comportano rischi specifici;
- effettuare **procedure di verifica** per assicurare che tutte le misure siano applicate ed efficaci.

Non vi sono, comunque, misure organizzative valide per ogni situazione: **la valutazione e la scelta delle misure da implementare dipende dalla modalità di gestione dello studio**.

Il GDPR statuisce che si debba tener conto *"dello* ***stato dell'arte*** *e dei* ***costi*** *di attuazione, nonché della natura, dell'oggetto, del contesto e delle* ***finalità del trattamento,*** *come anche del* ***rischio*** *di varia probabilità e gravità* ***per i diritti e le libertà delle persone*** *fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto* ***misure tecniche e organizzative adeguate*** *per garantire un livello di sicurezza adeguato al rischio".*

Come **esempi di misure tecniche** adeguate possono essere riprese le "misure di sicurezza minime" previste dall'allegato B del Codice della Privacy:

- **Autenticazione informatica** e gestione delle credenziali di autenticazione:
  1) i singoli **incaricati** devono essere dotati di **credenziali di autenticazione** (user id e password; otp…);
  2) assegnazione di un **user ID** identifica l'incaricato del trattamento ed è **personale**;
  3) la **password** deve essere conservata in luogo **non accessibile** ad alcuno tranne i soggetto ad essa afferente e deve essere composta da **almeno 8 caratteri** (maiuscole + minuscole+numeri+segni speciali) e non deve essere direttamente riferibile al soggetto;
  4) deve essere **modificata** al primo accesso e successivamente ogni 6 mesi o ogni 3 mesi per i dati particolari;
  5) le credenziali non utilizzate per oltre 6 mesi vanno disattivate;
- **Aggiornamento periodico** dell'ambito di trattamento;
- **Protezione degli strumenti elettronici**: lo studio deve censire i sistemi hardware e software e valutare la funzionalità:

1. Software:

- ✔ lo studio ad esempio deve essere dotato di **sistemi operativi aggiornati** e suscettibili di ricevere *patch* di aggiornamento (es. windows 2000; 2007 e vista non sono a norma);
- ✔ deve essere presente un **antivirus aggiornato** e deve essere effettuato con regolarità il ***backup*** almeno settimanalmente;

2. Hardware:

- ✔ devono essere dotati di un gruppo di continuità (garantire la resilienza) e di sistemi fisici antivirus (firewall);

- ✔ se i dati vengono mantenuti su un server fisicamente posto in studio verificare conformità dei locali;
- ✔ se i dati vengono mantenuti su un *cloud* di un'azienda terza sarà necessario contrattualizzare il terzo quale responsabile esterno del trattamento e verificare se i server su cui tali dati sono poggiati ha sede in UE o se l'azienda abbia aderito e attuato i principi di cui al GDPR;
- ✔ aggiornare il wi-fi di studio se ancora funzionate con tecnologia di accesso WEP (Wired Equivalent Privacy), protocollo datato e facilmente superabile (individuazione della password) con una minima conoscenza informatica: è preferibile il WPA2 piuttosto che i più vecchi standard WEP e WPA.

- Custodia di copie di sicurezza e **verifica periodica della corrispondenza e della funzionalità delle copie di backup** rispetto ai dati salvati al fine di verificare integrità e disponibilità dei dati;
- Tecniche di cifratura per i **dati "sensibili"** (sulla salute e la vita sessuale);
- Conservazione documentale informatica:

1) i documenti informatici e gli **atti sottoscritti digitalmente**, le **fatture elettroniche** trasmessi a mezzo PEC e le stesse PEC devono essere sottoposti a procedure di **conservazione documentale** in quanto, sia la firma digitale del sottoscrittore che le certificazioni apposte dal gestore PEC, sono soggette a scadenza;
2) sarà, pertanto, necessario dotarsi di uno spazio di archiviazione presso un **soggetto terzo in grado** di certificare la validità delle firme alla data di sottoscrizione;

- Dati trattati senza l'ausilio di strumenti elettronici (es. **fascicoli cartacei**) sarà necessario:

1) mantenere un archivio situato in **locali con accesso riservato** (senza accesso diretto dei clienti e dei terzi) e mantenuti in un armadio chiuso a chiave;
2) evitare che persone non autorizzate possano conoscere nomi di clienti o di terzi che eventualmente risultino dal contenitore, anonimizzando la copertina;

- Principio di minimizzazione (durata nel tempo della conservazione): i dati vanno conservati solamente per il tempo necessario, ovvero nel caso degli avvocati i **10 anni** previsti per legge dalla cessazione dell'incarico o dal passaggio in giudicato della causa.

IL REGISTRO DEI TRATTAMENTI

Il GDPR (art. 30) prevede che *"ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità"*.

Sebbene tale obbligo non si applichi di regola alle imprese o organizzazioni con meno di 250 dipendenti, il registro resta **necessario ove il trattamento** dei dati possa presentare un rischio per i diritti e le libertà dell'interessato, **non sia occasionale** o includa il trattamento di **categorie particolari di dati** (i dati "sensibili"), o i dati personali relativi a **condanne penali e a reati**.

Quindi, **gli avvocati** per la natura dei dati trattati **sono tenuti alla redazione e conservazione del Registro**.

In ogni caso, il **registro** dei trattamenti (elettronico o cartaceo) è fondamentale, sia per disporre di un quadro aggiornato dei trattamenti svolti, ma anche **per un eventuale** richiesta di supervisione e richiesta di **esibizione dal Garante**.
Serve a dimostrare che il Titolare o il Responsabile del trattamento si conforma al GDPR ed ha **funzione di**:

1) **censire** le banche dati e i **trattamenti** in essere;
2) **rappresentare l'organizzazione** sotto il profilo dell'attività di trattamento ai fini di informazione, consapevolezza e condivisione interna;
3) Costituisce **strumento di pianificazione e controllo** dei trattamenti per garantire la loro riservatezza e disponibilità;
4) **Riduce sprechi di tempo**, risorse, duplicazioni di informazioni;
5) **Riduce i rischi di trattamento illecito**.

DATA BREACH E SANZIONI

Il GDPR definisce la **violazione dei dati personali** come la *"**violazione di sicurezza** che comporta accidentalmente o in modo illecito la **distruzione**, la **perdita**, la **modifica**, la **divulgazione non autorizzata** o **l'accesso** ai dati personali trasmessi, conservati o comunque trattati".*

In caso di violazione dei dati personali, **il titolare del trattamento notifica la violazione all'autorità di controllo competente** senza ingiustificato ritardo e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, **a meno che sia improbabile che la violazione dei dati personali presenti un rischio** per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo **non** sia effettuata **entro 72 ore**, è **corredata dei motivi del ritardo**.

La notifica deve:
- **descrivere la natura della violazione** dei dati personali compresi, ove possibile, le **categorie** e il **numero** approssimativo di **interessati** in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il **nome e i dati di contatto del responsabile della protezione** dei dati **o di altro** punto di **contatto** presso cui ottenere più informazioni;
- descrivere le **probabili conseguenze** della violazione dei dati personali;
- descrivere **le misure adottate o di cui si propone l'adozione** da parte del titolare del trattamento per porre **rimedio** alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

In pratica, **in caso di *Data Breach* il titolare deve**:
- **compilare il registro** delle violazioni;
- **valutare l'impatto** della violazione: deve **notificare l'evento all'Autorità** salvo il caso in cui sia improbabile che la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati;
- **se è probabile che la violazione costituisca un rischio elevato** per i diritti e le libertà degli interessati **e il titolare non aveva adottato misure** tecniche e organizzative per proteggere i dati personali oggetto di violazione; né successivamente ha adottato misure in grado di scongiurare tale pericolo deve comunicare la violazione all'interessato.

Le **sanzioni** previste dal GDPR sono particolarmente elevate, ed arrivano a seconda delle violazioni **fino a 10.000.000 di euro o fino a 20.000.000 di euro**, o per le imprese, **fino al 2% o fino al 4 % del fatturato**.
In ogni caso, le sanzioni date dal GDPR sono fissate nel massimo edittale lasciando **al Garante locale** la **determinazione** delle **misure minime che dovranno essere proporzionate e dissuasive** tenuto conto del contesto di applicazione e dell'impatto delle violazioni contestate.

PROFILI DEONTOLOGICI DEL GDPR

Il **GDPR,** oltre a contenere sanzioni amministrative proprie, può incidere anche in **ambito deontologico** e di responsabilità professionale.

In particolare, l'art. 13 del Codice Deontologico Forense prevede che *"l'avvocato è tenuto, nell'interesse del cliente e della parte assistita, alla **rigorosa osservanza del segreto professionale** e al massimo **riserbo** su fatti e circostanze in qualsiasi modo apprese nell'attività di rappresentanza e assistenza in giudizio, nonché nello svolgimento dell'attività di consulenza legale e di assistenza stragiudiziale e comunque per ragioni professionali".*

Analogamente, l'art. 28 dispone come *"è **dovere,** oltre che diritto, primario e fondamentale dell'avvocato **mantenere il segreto e il massimo riserbo** sull'attività prestata **e su tutte le informazioni che gli siano fornite dal cliente** e dalla parte assistita, nonché su quelle delle quali sia venuto a conoscenza in dipendenza del mandato".*

Appare evidente come, per rispettare tali norme deontologiche, l'avvocato oggi debba rispettare la normativa prevista dal GDPR.

DISCLAIMER:

La presente guida è aggiornata al momento della sua pubblicazione.

Ciò nonostante, la natura stessa degli argomenti trattati esclude la possibilità di controllare tutte le fonti esistenti e l'autore non può fornire alcuna garanzia in merito all'affidabilità ed all'esattezza delle notizie riportate e declina pertanto ogni responsabilità per qualsiasi danno, diretto, indiretto, incidentale e consequenziale legato all'uso, proprio o improprio delle informazioni contenute in questo vademecum, ivi inclusi, senza alcuna limitazione, la perdita di profitto, l'interruzione di attività aziendale o professionale, la perdita di programmi o altro tipo di dati ubicati sul sistema informatico dell'utente o altro sistema,e ciò anche qualora l'autore fosse stato espressamente messo al corrente della possibilità del verificarsi di tali danni.

Le guide del
Movimento
Forense
Triveneto