Ordine degli Avvocati di Trani

ASSOCIAZIONE AVVOCATI ANDRIESI

AAA

LINEE GUIDA

per lo Studio Legale
alle Misure Minime di Sicurezza
ed alla redazione del
Documento Programmatico sulla Sicurezza
dettati dalla nuova disciplina sul
Trattamento dei Dati Personali
(D. Lgs. 30 giugno 2003 n, 196)

INDICE

Prefazione

Per un inquadramento delle problematiche relative agli adempimenti che gravano sull'avvocato nell'esercizio dell'attività professionale imposti dal Codice della Privacy, si è pensato di redigere il presente opuscolo contenente suggerimenti in materia di sicurezza con allegati modelli, schemi e tabelle.
Ai fini di una consultazione del materiale attraverso i sistemi informatici è stato realizzato un cd contenente le linee guida; i modelli; la normativa di riferimento, programmi ed utilità.
Saremmo grati ai colleghi di tutto il foro per i suggerimenti e gli spunti di riflessione che vorranno dare per un miglioramento ed una integrazione delle presenti linee guida.
Certi di avere contribuito a fornire a tutti gli iscritti una serie di suggerimenti per districarsi tra gli adempimenti posti dalla normativa Vi auguriamo un buon lavoro.

Avv. Francesco Tedeschi
Presidente Associazione Avvocati Andriesi
Redattore delle linee guida

Avv. Bruno Logoluso
Presidente Consiglio dell'Ordine
degli Avvocati di Trani

Premessa

Il legislatore del 2003 nell'adottare una normativa a tutela dei dati personali e sensibili ha inteso riordinare la materia dettando una disciplina unitaria alla quale ha dato il nome di Codice in materia di protezione dei dati personali
Tuttavia prima di affrontare le novità e le problematiche derivanti dall'applicazione della disciplina con particolare riferimento agli obblighi ed agli adempimenti nell'esercizio dell'attività forense è opportuno effettuare una premessa di carattere generale sul tema della tutela della privacy.
I dati personali sono elementi indefettibili che ogni avvocato tratta in ragione dell'attività che svolge.
Molto spesso non si attribuisce molta attenzione a tale aspetto perché forse non ci si rende conto che ogni elemento che vale ad identificare il cliente costituisce un *dato personale* e nell'ipotesi, ad esempio, di elementi relativi allo stato di salute del cliente, il relativo dato costituisce *dato sensibile*.
Le norme di deontologia professionale impongono all'avvocato un dovere di segretezza che, ovviamente, si estende a tutto ciò che riguarda non solo l'affare affidato dal cliente, ma anche tutti gli elementi identificativi del cliente, al fine di evitare di dare pubblicità esterna alle vicende di carattere contenzioso che lo coinvolgono.
L'art. 9 del Codice deontologico detta precise regole di segretezza e riservatezza.
Il nuovo Codice sulla Privacy ha introdotto una serie di adempimenti specifici che ciascun operatore deve adottare per garantire la sicurezza di tutti i dati del cliente.
Le misure che il codice della privacy impone sono dirette a prevenire il rischio di diffusione di dati personali dei clienti con particolare attenzione ai dati trattati con strumenti informatici.
La tutela della riservatezza è un concetto che ci rinviene dalle normative di common law ed è stato recepito nella Carta Fondamentale dei diritti fondamentali dell'Unione Europea (cd. Carta di Nizza) e da numerose Direttive CE e Raccomandazioni del Consiglio d'Europa.
Il diritto alla riservatezza trova il suo riconoscimento nel ns. ordinamento anche nella Carta Costituzionale laddove l'art. 2 riconosce e garantisce i diritti inviolabili dell'uomo e l'art. 13 sancisce l'inviolabilità della libertà personale. Tra i diritti inviolabili dell'uomo, in una visione evolutiva, devono ricomprendersi i diritti connessi con la riservatezza dei dati personali che lo riguardano. La libertà personale comprende anche il diritto alla riservatezza dei dati personali e, conseguentemente anche il diritto al riconoscimento ed alla pretesa che i dati personali siano tutelati attraverso meccanismi di difesa degli stessi.
In linea di principio l'art. 1 del Codice della Privacy sancisce i diritto alla protezione dei propri dati personali.
Tuttavia non tutti i dati personali hanno eguale diritto di protezione, infatti, i dati pubblici quali la data di nascita e quant'altro reperibile in pubblici registri, non richiedono una particolare cautela e/o tutela.
Il legislatore non si è preoccupato di dare qualificazione giuridica al dato ed in particolare se inquadrarlo tra i beni materiali o immateriali.
Il dato personale se non può inquadrarsi in un bene immateriale va considerato come un fattore conoscitivo che un soggetto ha di un altro soggetto. Orbene se l'acquisizione di tale dato è avvenuto legittimamente, attraverso una procedura consentita dalla legge, non par dubbio che la detenzione di tale dato non è vietato dal Codice della Privacy. Il Codice della Privacy non vieta la detenzione dei dati, ma il suo utilizzo e stabilisce che i dati debbono essere protetti e non divulgati se non per finalità connesse con l'esercizio di una attività lecita e, per taluni dati la circolazione di essi può avvenire solo con il consenso dell'interessato.
L'esercizio della professione forense comporta necessariamente la detenzione di dati personali di clienti e di terzi finalizzati all'esercizio dell'attività di tutela degli interessi del cliente.
Il Codice della Privacy ed i provvedimenti del Garante sono finalizzati a rendere l'esercizio della professione forense più aderente alle normative europee e di oltre oceano in tema di diritto alla riservatezza dei dati che il professionista detiene in ragione dell'attività che svolge.

Ad una superficiale lettura del Codice della Privacy può sembrare che la normativa sia tesa a rendere più onerosa la gestione dell'attività interna dello Studio Legale.
Invero se si pone attenzione a tutti gli adempimenti previsti dalla normativa in esame è facile osservare che, in gran parte, gli adempimenti che vengono fissati nel Codice della Privacy dovrebbero essere già stati adottati negli Studi Legali. Infatti, ad esempio, la dotazione di protezione di accesso al computer è una norma di buon senso che ciascun professionista dovrebbe già avere adottato e molti professionisti già adottano cautele per disciplinare l'accesso ai contenuti di alcuni atti di clienti e quindi ai dati ivi contenuti.
In ogni caso bisogna cambiare l'approccio verso la materia ed ipotizzare gli adempimenti come adempimenti di routine che si adottano al momento della acquisizione del conferimento dell'incarico da parte del cliente. Infatti, quando un cliente affida un incarico si è soliti inserire i documenti ricevuti in una cartellina sulla quale viene indicato il nome del cliente e la controparte, i dati personali del cliente vengono inseriti in una agenda che consenta il suo facile reperimento, e conseguentemente poi si è soliti provvedere a collocare il fascicolo di ufficio in uno schedario non certo accessibile a chiunque frequenti lo Studio Legale. Con il Codice della Privacy tali adempimenti non sono appesantiti ma sono soltanto specificatamente disciplinati. Il professionista dovrà solo cambiare leggermente il suo modus operandi, provvedendo a seguire alcune regole di prudenza che gli eviteranno di essere esposto al rischio di arrecare danno al cliente e di farsi muovere un rimprovero di scarsa affidabilità.
Purtroppo la sicurezza viene spesso percepita in senso negativo perché tesa a determinare interferenza con le consolidate procedure di gestione dello Studio ed aumentare il lavoro con adempimenti supplementari.
Tuttavia la sottovalutazione del fattore sicurezza aumenta la vulnerabilità dei sistemi di protezione non solo dei dati ma dell'intero processo produttivo dello Studio.
In una ottica di strategia a medio-lungo termine una maggiore attenzione al fattore sicurezza dei dati personali costituisce uno strumento di potenziamento e di acquisizione di clientela perché le modalità adottate per garantire la sicurezza dei dati detenuti per conto del cliente costituirà un fattore determinante di scelta del professionista. Infatti, nel Regno Unito si è sviluppata una normativa standard denominata BS 7799 ovvero ISO 17799 costituente in pratica un codice per la gestione della sicurezza delle informazioni adottato a livello internazionale. Il rispetto di tali standards costituisce un fattore di qualità per coloro che dimostrano di esservi adeguati.
Pertanto un cambiamento della mentalità in tema di sicurezza dei dati personali non potrà portare benefici all'esercizio della professione legale.

DATI E TRATTAMENTO

Al fine di inquadrare la materia è opportuno preliminarmente soffermarsi sul concetto di dato personale così come inteso dal legislatore della Privacy ed il suo trattamento

DATI PERSONALI

Il primo comma dell'art. 4 individua e definisce i dati personali ed il loro trattamento.

a) trattamento.

Per trattamento s'intende qualunque operazione o complesso di operazioni, effettuati sui dati anche senza l'ausilio di strumenti elettronici, anche se non registrati in una banca di dati, concernenti:

- **raccolta**
- **registrazione**
- **organizzazione**
- **conservazione**
- **consultazione**
- **elaborazione**
- **modificazione**
- **selezione**
- **estrazione**
- **raffronto**
- **utilizzo**
- **interconnessione**
- **blocco**
- **comunicazione**
- **diffusione**
- **cancellazione**
- **distruzione**

Come si può agevolmente vedere si tratta di uno spettro ampio di attività che comprende ogni ipotizzabile operazione su dati di clienti o di terzi che uno Studio Legale detiene e che prescinde dal tipo di organizzazione dello Studio Legale (informatizzata o meno).

b) dato personale

Per dato personale qualunque informazione relativa a

- **persona fisica**
- **persona giuridica**
- **ente od associazione**

identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Il Codice della Privacy attribuisce importanza ad ogni informazione che possa consentire l'individuazione del soggetto cui l'informazione si riferisce, anche attraverso elementi apparentemente esterni al soggetto quali fotografie, filmati, estremi di documenti di identità – patente; PIN; ID; suoni; impronte digitali; caratteristiche biometriche; caratteri alfanumerici ecc. Tutto ciò che potrebbe consentire di individuare un soggetto è dato personale.

c) dato identificativo

Il dato identificativo è il dato personale che consente l'identificazione diretta del soggetto quale il nome, il cognome la sua data di nascita il suo codice fiscale

d) dato sensibile

Per dato sensibile si intende il dato personale che consente di individuare di un soggetto:

- **l'origine razziale ed etnica;**
- **le convinzioni religiose, filosofiche o di altro genere;**
- **le opinioni politiche;**
- **l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale,**
- **lo stato di salute**
- **la vita sessuale**

Trattasi di dati personali estremamente delicati per i quali il Codice della Privacy prevede nella generalità dei casi l'obbligo del trattamento solo previo consenso scritto dell'interessato e previa autorizzazione del Garante salvo quanto previsto dall'art. 26 punto 4) del Codice della Privacy

e) dato giudiziario
Trattasi di quei dati personali che sono diretti a rivelare:

- **le iscrizioni nel casellario giudiziale delle condanne penali; delle pene inflitte; delle pene convertite e quant'altro venga iscritto nel casellario giudiziale ad eccezione delle sentenze dichiarative di fallimento e dei provvedimenti di interdizione, inabilitazione e revoca:**
- **le sanzioni amministrative dipendenti da reato**
- **i carichi pendenti**
- **la qualità di imputato o indagato**

Per questi dati è consentito il trattamento soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichi le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

SOGGETTI

Nell'ambito delle definizioni il Codice della Privacy individua una serie di categorie di soggetti ai quali viene attribuita rilevanza a seconda del diverso rapporto che questi hanno con i dati personali.

a) Titolare
Il Codice della Privacy definisce il titolare del trattamento dei dati personali come colui che nell'ambito della organizzazione dello Studio Legale, anche insieme ad altro soggetto titolare, abbia il potere di assumere le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

b) Responsabile
Il Responsabile del trattamento dei dati personali è individuato in colui che è preposto dal titolare al trattamento dei dati.
In uno Studio Legale di piccola – media dimensione la figura del titolare e quella del responsabile coincidono. Infatti, una distinzione dei ruoli può ipotizzarsi in una organizzazione che si sviluppi nel territorio in più centri di aggregazione, onde si rende necessario per ogni sede individuare il responsabile del trattamento. Si immagini uno Studio Legale che abbia più sedi dislocate nel territorio nazionale o estero. Orbene in tale caso il Titolare ed il Responsabile del trattamento dei dati personali potranno essere soggetti diversi e vi potranno essere più responsabili

c) Incaricato
Per incaricato al trattamento dei dati si intende colui che materialmente provvede ad effettuare le operazioni di trattamento dei dati.

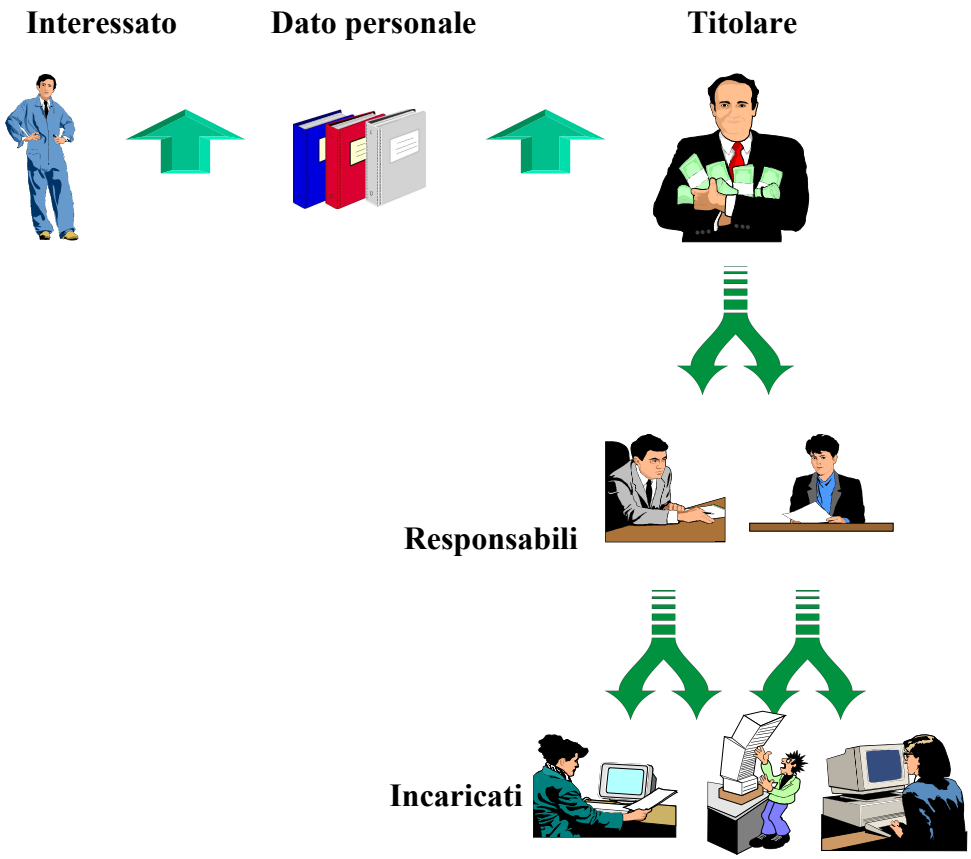
d) Interessato
L'interessato al trattamento dei dati è quel soggetto cui si riferiscono i dati oggetto di trattamento. L'interessato non solo potrà essere colui che spontaneamente ha fornito il dato personale ma anche colui i cui dati sono conosciuti o posseduti dallo Studio Legale in funzione dell'esercizio di difesa del cliente. Pertanto l'interessato non è solo il cliente ma anche il terzo, la controparte, il giudice, il consulente di parte o d'ufficio ovvero chiunque del quale si detengono dati.

e) Rappresentante del Titolare del trattamento.
Tale figura individuata nell'art. 5 del Codice della Privacy riguarda le ipotesi di strutture organizzate su un ambito territoriale internazionale laddove il Titolare designa un suo rappresentante per l'Italia. Tale figura non sarà oggetto di interesse nel presente lavoro perché trattasi di ipotesi riguardante strutture organizzative statisticamente ridotte nel territorio locale.

Se si pone attenzione alle definizioni descritte nell'art. 4 del Codice della Privacy si potrà notare che mentre il titolare, il responsabile e l'interessato possono essere indifferentemente sia persone fisiche che giuridiche, enti ed associazioni; l'incaricato può essere solo una persona fisica. Infatti colui che materialmente tratta i dati personali su istruzione del responsabile non può che essere una persona fisica. Al contrario, il responsabile può essere anche un soggetto giuridico impersonale quale una società che impartisce le regole cui gli incaricati debbono attenersi.
Tuttavia la concreta responsabilità sulla adozione delle misure ed i profili di responsabilità penale o amministrativi saranno sempre incidenti sui legali rappresentanti dell'ente che hanno il potere gestorio degli affari; le eventuali responsabilità civili graveranno sul titolare o responsabile qualunque sia la sua configurazione giuridica.

Uno schema potrà agevolmente far comprendere i rapporti tra interessato, dato personale e soggetti indicati nel Codice della Privacy.

RAPPORTI TRA DATO PERSONALE E SOGGETTI



DIRITTI DELL'INTERESSATO.

Il Codice della Privacy ha individuato i diritti dell'interessato.

I diritti dell'interessato si possono distinguere in

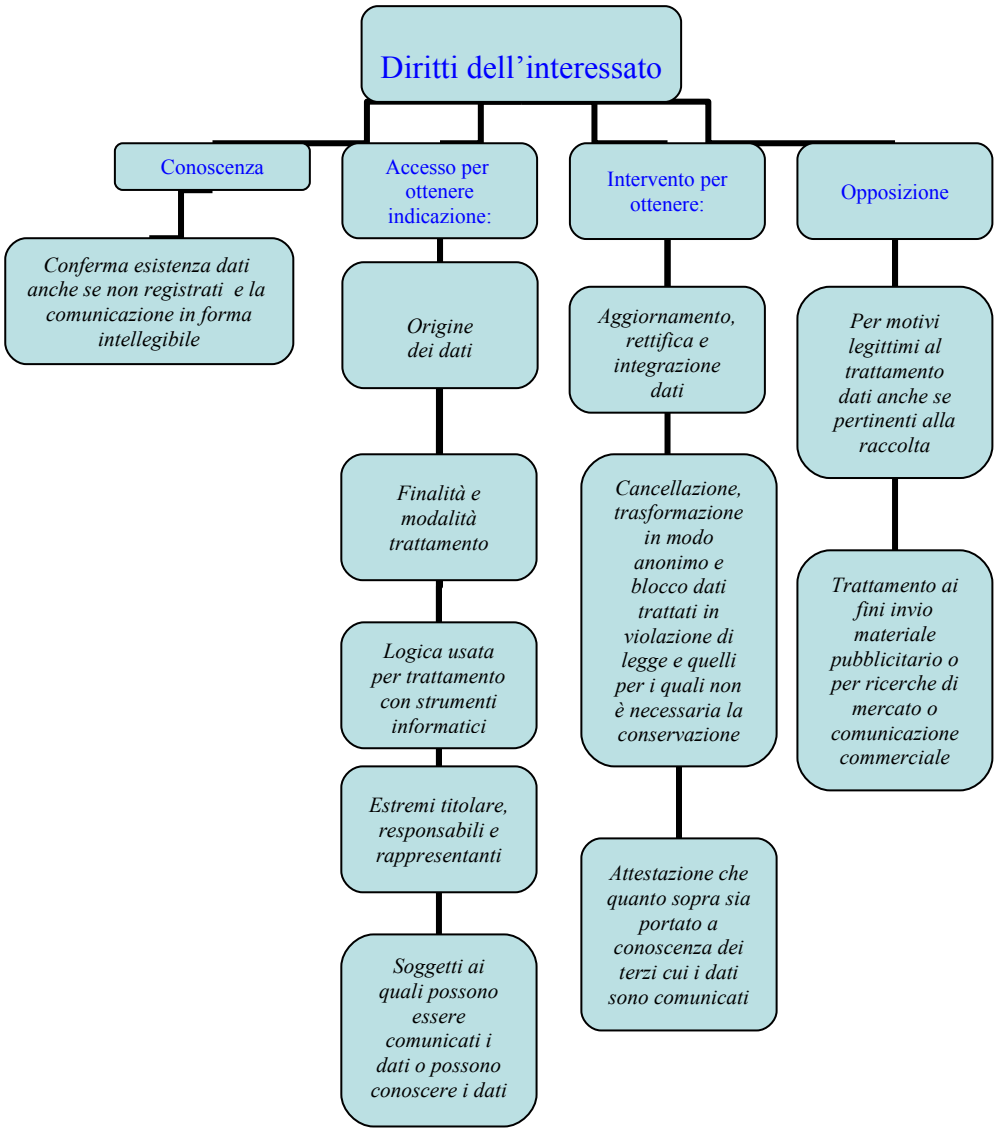
- **diritti di conoscenza;**
- **diritti di accesso;**
- **diritti di intervento**
- **diritti di opposizione**.

L'ampiezza dei diritti riconosciuti all'interessato rendono comprensibile e giustificabili tutte le disposizioni contenute nel Codice della Privacy dirette ad imporre al titolare del trattamento una serie di adempimenti finalizzati alla tutela ed alla salvaguardia dei dati personali detenuti.

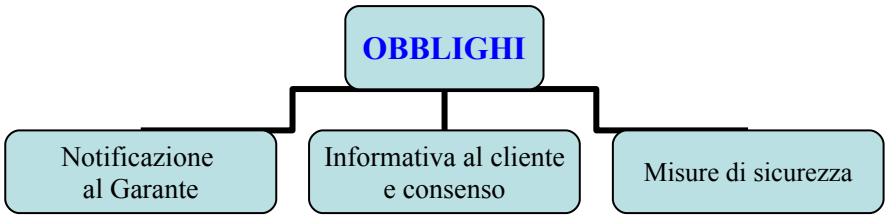
In buona sostanza l'adozione delle misure di sicurezza dei dati, oltre che essere giustificata dagli obblighi imposti dal Codice Deontologico e da regole di buon senso, sono essenzialmente dirette a consentire la tutela dei diritti dell'interessato.

L'art. 7 del Codice della Privacy indica in modo preciso i diritti dell'interessato secondo la distinzione sopra riportata

Uno schema può essere agevole per individuare i diritti dell'interessato a seconda del tipo di diritto riconosciutogli dal Codice della Privacy.



Ai diritti dell'interessato corrispondono obblighi a carico del titolare del trattamento dei dati.
Gli obblighi e conseguentemente gli adempimenti a carico del Titolare a tutela dei diritti dell'interessato possono così sintetizzarsi



Notificazione al Garante

I professionisti del settore legale sono esentati dalla notificazione del trattamento al Garante prevista dall'art. 37 Codice della Privacy.
Il Garante della Privacy ha emesso autorizzazione generale n. 04 del 2004 per il trattamento dei dati sensibili da parte dei professionisti
Conseguentemente l'Avvocato titolare del trattamento è esentato dalle comunicazioni al Garante per il trattamento dei dati sensibili.
Il Codice della Privacy prevede l'obbligo della notificazione al Garante nelle ipotesi previste dall'art. 37 comma 1° del Codice della Privacy e, per ciò che può riguardare la professione forense, specificatamente relative a:

- **dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;**
- **dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.**

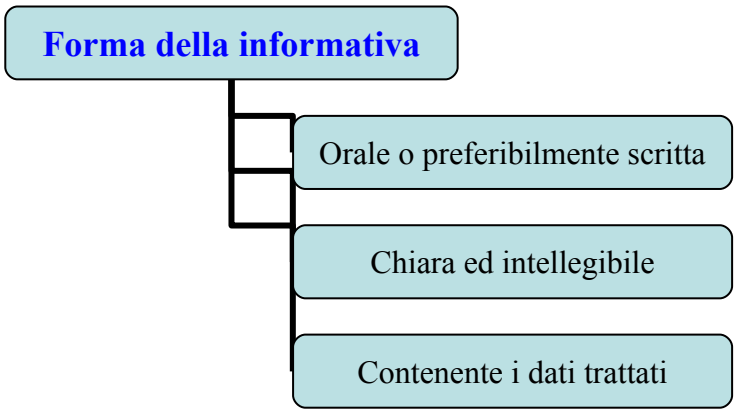
Tuttavia il Garante della Privacy ha emesso in data 31/03/2004 un provvedimento ai sensi del secondo comma dell'art. 37 avente valenza generale, pubblicato sulla Gazzetta Ufficiale n. 81 del 06/04/2004, con il quale sottrae dall'obbligo della notificazione al Garante il trattamento dei dati sensibili avente ad oggetto i trattamenti di dati genetici o biometrici effettuati nell'esercizio della professione di avvocato, in relazione alle operazioni e ai dati necessari per svolgere le investigazioni difensive di cui alla legge n. 397/2000, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria. Ciò sempre che il diritto sia di rango almeno pari a quello dell'interessato e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento.
Analogamente sono sottratti all'obbligo della notificazione i dati registrati in banche di dati utilizzate in rapporti con l'interessato di fornitura di beni, prestazioni o servizi, o per adempimenti contabili o fiscali, anche in caso di inadempimenti contrattuali, azioni di recupero del credito e contenzioso con l'interessato.
Residua l'obbligo della notificazione al Garante solo nell'ipotesi in cui lo Studio Legale detenga e tratti quei dati con strumenti elettronici per fini diversi dall'attività di indagini difensive ovvero per fini diversi dall'esercizio della difesa del cliente in sede giudiziaria.

INFORMATIVA E CONSENSO

L'informativa è disciplinata dall'art. 13 del Codice della Privacy e costituisce un momento fondamentale del trattamento dei dati personali dell'interessato.
L'informativa ha la specifica funzione di consentire all'interessato di conoscere in via preventiva se e con quali modalità i propri dati personali vengono trattati dallo Studio Legale anche al fine di consentirgli di esercitare i diritti che gli sono concessi dall'art. 7 del Codice della Privacy.
Altresì l'informativa consente di far verificare all'interessato se sono rispettate le modalità di trattamento dei dati che lo riguardano.
L'informativa impone anche un onere di aggiornamento dei dati personali trattati
Il legislatore della Privacy ha strutturato l'informativa in modo tale da prevedere con particolarità

- **la forma**
- **il contenuto**
- **consenso**
- **le esenzioni dal consenso**

La forma dell'informativa può essere orale o scritta.
Tuttavia è opportuno che la stessa sia manifestata per iscritto con una comunicazione da inviarsi o consegnarsi all'interessato ovvero anche attraverso una forma che renda noto all'interessato il contenuto dell'informativa, ad esempio, attraverso la sua libera distribuzione all'interno dello Studio ovvero con un cartello appeso nello Studio.
Rimane preferibile la forma scritta comunicata o consegnata al cliente prima del trattamento dei dati al fine di evitare contestazioni e responsabilità.
Pertanto la forma della informativa può così riassumersi



L'informativa deve essere resa all'interessato prima del trattamento.
Il Parere del Garante in data 03/06/2004 evidenzia che l'informativa va resa nota al momento del conferimento dell'incarico.
Invero i dati trattati in uno Studio Legale non sono solo quelli relativi al cliente ma anche quelli relativi a soggetti diversi dal cliente.
Ad una lettura dell'art. 1 del Codice della Privacy la locuzione usata di "*chiunque*" fa propendere per l'estensione della informativa nei confronti di tutti coloro i cui dati vengono trattati nello Studio.

Si ritiene che l'ipotesi di dati relativi a soggetti diversi dal cliente rientri tra le ipotesi indicate nel comma 4 dell'art. 13 che non si applica quando

- **i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;**
- **i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;**

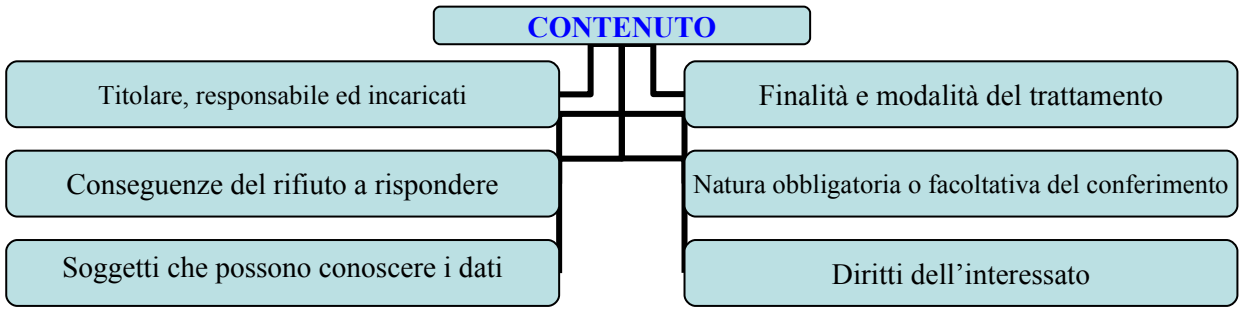
Un problema si pone allorquando si trattano i dati di terzi nell'ambito di un'attività di tutela del cliente in ambito stragiudiziale.
Il Garante nel parere del 03/06/2004 ha inteso limitare le eccezioni all'obbligo di informativa alle sole ipotesi di esercizio di difesa in sede giudiziaria.
Non par dubbio che una interpretazione restrittiva comprimerebbe non poco l'esercizio del diritto di difesa del cliente allorquando per il suo esercizio si renda necessario trattare dati di controparti. Si pensi all'ipotesi di difesa di un cliente in materia di infortunistica o di lavoro laddove i dati di terzi-controparti siano trattati nella fase antecedente la fase giudiziaria. Si pensi all'ipotesi in cui si renda necessario proporre azione cautelare ante causam: in tal caso i dati della controparte sono trattati prima dell'inizio del giudizio e la comunicazione dell'informativa potrebbe pregiudicare gli interessi del cliente.
Il Garante nel fornire il Parere del 03/06/2004 sembra non essersi reso conto delle conseguenze di una interpretazione restrittiva dell'art. 13 del Codice della Privacy.
Invero tale interpretazione restrittiva espone il Codice della Privacy ad una censura di legittimità costituzionale per violazione dell'art. 3, 24 e 76 della Costituzione.
Infatti, l'attività stragiudiziale costituisce una forma di tutela dei diritti del cliente e nell'esercizio del diritto di difesa del cliente rientra anche il trattamento dei dati di terzi. L'informativa resa nota ai terzi del trattamento dei loro dati per motivi connessi con l'esercizio del diritto di difesa di un proprio cliente potrebbe ragionevolmente ledere i diritti del cliente.
Pertanto l'art. 13 del Codice della Privacy sarebbe in contrasto:

- con l'art. 3 della Costituzione laddove pone in una situazione di disparità coloro che esercitano il loro diritto in sede giudiziaria da quello che esercitano il loro diritto in sede stragiudiziale;
- con l'art. 24 della Costituzione in una sua interpretazione evolutiva laddove il diritto di difesa non si esercita solo in ambito giudiziario e laddove l'esercizio del diritto di difesa in ambito giudiziario può o deve essere preceduto da una fase stragiudiziale (si pensi alle controversie di lavoro ove è prevista una fase obbligatoria di conciliazione stragiudiziale);
- con l'art. 76 della Costituzione per violazione della legge delega n. 676/1996. L'art. 1 della legge delega n. 676/1996 imponeva al Governo l'emanazione di una normativa in materia di trattamento dei dati personali che garantisse la piena attuazione dei princìpi previsti dalla legislazione in materia di dati personali nell'ambito dei diversi settori di attività, nel rispetto dei criteri direttivi e dei princìpi della normativa comunitaria. Orbene l'art. 20 della Direttiva CE n. 54/2001 ha espressamente previsto una deroga all'obbligo di informazione da fornire all'interessato (art 12 del predetto Regolamento CE) nell'ipotesi di tutela dell'interessato o dei diritti e delle libertà altrui (cliente)

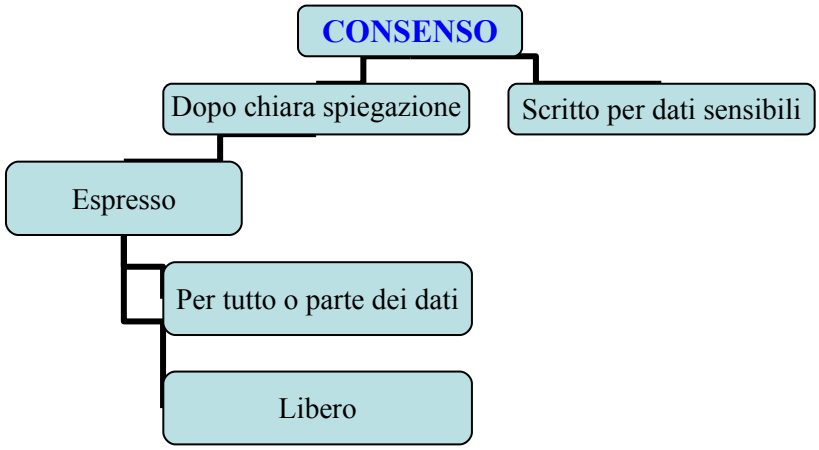
Allo stato l'interpretazione fornita dal Garante, attraverso il suo parere del 03/06/2004 , imporrebbe l'onere della informativa ai terzi nell'ipotesi di esercizio del diritto di difesa in fase stragiudiziale.

Il **contenuto** dell'informativa è indicato nell'art. 13 del Codice della Privacy.

Tra gli elementi che devono essere contenuti nell'informativa vi è l'indicazione delle finalità e *modalità* del trattamento.
Orbene l'art. 11 del Codice della Privacy indica le modalità con le quali devono essere trattati i dati; ne conseguirebbe che nell'informativa sarebbe sufficiente dire che i dati verranno trattati secondo le modalità indicate nell'art. 11 del Codice della Privacy.
Si ritiene che tale rimando non sia sufficiente perché altrimenti non ci sarebbe alcuna necessità di prevedere tale indicazione nell'informativa.
Pertanto, poiché lo scopo dell'informativa è quello di fornire la più ampia informazione circa il trattamento dei dati che lo Studio Legale effettua, è necessario indicare nell'informativa le modalità concrete con le quali verrà trattato il dato: indicazione degli strumenti attraverso i quali si tratterà il dato personale, il tipo di supporti (informatizzati o meno), programmi, le procedure di conservazione e diffusione attraverso l'indicazione dei soggetti che potranno avere conoscenza dei dati personali (controparti, consulenti, uffici giudiziari, testimoni, terzi intervenuti ecc.)
Pertanto il contenuto della informativa può così riassumersi



La disciplina del consenso è regolata dal Capo III del Titolo III del Codice della Privacy.
In linea generale l'art. 23 del Codice della Privacy indica le modalità con le quali deve essere acquisito il consenso che possono così schematizzarsi



L'art. 24 del Codice della Privacy indica i casi per i quali il trattamento dei dati può essere effettuato senza il consenso, specificandone le modalità.
Il Garante con il parere espresso in data 03/06/2004 ha distinto le ipotesi di esercizio del diritto di difesa in sede giudiziaria dall'attività di difesa in ambito stragiudiziale.
Nell'ipotesi di esercizio del diritto di difesa in sede giudiziaria l'esenzione dal consenso potrà essere escluso in determinate ipotesi.

Di seguito si sintetizza il parere del Garante sulle ipotesi di esenzione dal consenso per tale ipotesi

	Cliente		Terzi	
Dati	**Consenso**	**Condizioni**	**Consenso**	**Condizioni**
Comuni	No		No	Indagini difensive; difendere diritto in sede giudiziaria e limitatamente per tali finalità salvo utile applicazione altri presupposti da art. 24 (dati pubblici ovvero obblighi di legge ecc.)
Sensibili	No	Indagini difensive; difendere diritto in sede giudiziaria e limitatamente per tali finalità	No	Strettamente indispensabile per eseguire specifiche prestazioni professionali richieste dai clienti per scopi legittimi purchè pertinenti e non eccedenti rispetto agl incarichi ricevuti
Rivelatori stato di salute e vita sessuale	No	Diritto fatto valere è di pari rango a quello dell'interessato (diritto personalità o altro diritto o libertà fondamentale. Rispetto prescrizioni Autorizzazione Generale n. 2/2004	No	Diritto fatto valere è di pari rango a quello dell'interessato (diritto personalità o altro diritto o libertà fondamentale. Rispetto prescrizioni Autorizzazione Generale n. 2/2004
Giudiziari	No	Rispetto prescrizioni Autorizzazione Generale n. 7/2004	No	Rispetto prescrizioni Autorizzazione Generale n. 7/2004

Per **l'attività stragiudiziale** il Garante ha precisato nel suo parere del 03/06/2004 che non sono applicabili le eccezioni previste dal Codice della Privacy per gli obblighi di informativa e consenso salvo per quanto riguarda i dati comuni per i quali potrà farsi utile applicazione di altri presupposti equipollenti al consenso (dati relativi ad attività economiche, adempimento di obblighi di legge ecc.) ed in particolare:

- Per i **dati comuni** il consenso del cliente non è richiesto secondo quanto sopra esposto ed alle condizioni sopra indicate.
- Il trattamento dei dati comuni di soggetti diversi dal cliente, nel caso in cui non possa applicarsi uno degli altri presupposti di cui all'art. 24 del Codice (ad esempio, dati "pubblici"), deve avvenire con il consenso dell'interessato
- Per i **dati sensibili** il trattamento richiede il consenso scritto dell'interessato. Per quanto riguarda l'autorizzazione del Garante, opera l'autorizzazione generale n. 4/2004. L'incarico dal professionista deve rientrare tra quelli che quest'ultimo può eseguire in base all'ordinamento professionale di riferimento.

- Per i **dati idonei a rivelare lo stato di salute e la vita sessuale** analogamente a quanto già accennato, il relativo trattamento dei dati richiede il consenso scritto dell'interessato e deve essere effettuato anche nel rispetto dell'autorizzazione generale n. 2/2004.
- Per i **Dati giudiziari** valgono le considerazioni sopra esposte

In allegato è riportato un modello di informativa da sottoporre all'attenzione dell'interessato.

MISURE DI SICUREZZA

Prima di affrontare il problema delle misure di sicurezza, è opportuno soffermarsi brevemente sul concetto di sicurezza.
Si pensa alla sicurezza ogni qualvolta si pone attenzione al rischio, al pericolo di perdita o lesione di un bene materiale o immateriale.
Lo sviluppo tecnologico e l'evoluzione del pensiero giuridico volto al riconoscimento di nuovi diritti e di tutela degli stessi in vari ambiti, hanno determinato maggiore attenzione al fattore prevenzione ed hanno impresso maggiore impulso all'individuazione di strumenti volti a prevenire perdite o lesioni dei diritti.
Si pensi all'evoluzione della tecnologia nel campo della motorizzazione. Le automobili di qualche anno fa erano poco attente a strumenti di prevenzione del rischio "impatto da scontro"; oggi ogni auto è dotata di air bag ed il rischio di lesioni determinate da uno scontro è limitato.
La maggiore attenzione rivolta alla tutela di riservatezza dei dati personali ed al loro utilizzo solo a precise condizioni, ha determinato la necessità di individuare gli strumenti per prevenire il rischio di loro perdita o loro diffusione e/o uso indiscriminato.
L'insieme degli strumenti rivolti alla protezione dei dati personali sono le misure di sicurezza.

Misure di sicurezza idonee.

Il legislatore della Privacy ha introdotto il tema delle misure di sicurezza nel Titolo V del Codice, operando una distinzione tra misure di sicurezza (Capo I) e misure minime di sicurezza (Capo II)
Sul tema l'art. 31 individua l'obbligo di sicurezza dei dati personali attraverso la loro custodia e controllo, *anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento in modo da ridurre al minimo, mediante l'adozione di* ***idonee*** *e preventive misure di sicurezza, i rischi di distruzione o perdita, anche se accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.*
Il Codice della Privacy individua nel capo II le misure minime di sicurezza fissando la soglia minima degli strumenti da adottare per la sicurezza dei dati, operando una distinzione tra il trattamento dei dati con strumenti elettronici (art. 34) e trattamento senza l'uso degli strumenti elettronici (art. 35)
Ad una lettura comparata delle due disposizioni di legge si nota una differenziazione tra misure minime e misure idonee
Da un punto di vista strettamente tecnico non ci sono differenze tra l'una e l'altra ipotesi perché una misura tecnica minima è sempre una misura tecnicamente idonea.
Da un punto di vista giuridico la distinzione è determinata dalle diverse conseguenze derivanti dalla mancata adozione dell'una o dell'altra regola.
Ne consegue che la distinzione tra misure idonee e misure minime è fondamentale ai fini della individuazione del livello di responsabilità relativo alle conseguenze in caso di violazione dell'una o dell'altra prescrizione.
Sinteticamente possono così distinguersi le due ipotesi

Violazione	Misure minime	Misure idonee
Conseguenze	Reato previsto dall'art. 169 del Codice	Responsabilità ex art. 15 del Codice

Non si può prescindere dall'adottare misure idonee individuate alla luce degli strumenti che il progresso tecnologico offre in via evolutiva.
Infatti, il predetto art. 15 del Codice della Privacy grava il titolare del trattamento di una responsabilità ai sensi dell'art. 2050 e 2059 c.c. nell'ipotesi in cui il danno all'interessato sia provocato a causa della mancata adozione di misure idonee di sicurezza.

Vi è una parte della dottrina e della giurisprudenza che ritiene esistente una presunzione di responsabilità in capo al titolare del trattamento sul quale grava l'onere di dimostrare di avere adottato tutte le misure idonee così come esistenti alla luce del progresso tecnologico per evitare la causazione del danno.
La presunzione di responsabilità contemplata dalla norma dell'art. 2050 c.c. per le attività pericolose può essere vinta solo con una prova particolarmente rigorosa, essendo posto a carico dell'esercente l'attività pericolosa l'onere di dimostrare l'adozione di "tutte le misure idonee ad evitare il danno": pertanto non basta la prova negativa di non aver commesso alcuna violazione delle norme di legge o di comune prudenza, ma occorre quella positiva di aver impiegato ogni cura o misura atta ad impedire l'evento dannoso, di guisa che anche il fatto del danneggiato o del terzo può produrre effetti liberatori solo se per la sua incidenza e rilevanza sia tale da escludere, in modo certo, il nesso causale tra attività pericolosa e l'evento e non già quando costituisce elemento concorrente nella produzione del danno, inserendosi in una situazione di pericolo che ne abbia reso possibile l'insorgenza a causa dell'inidoneità delle misure preventive adottate. (Cassazione civile, sez. III, 29 aprile 1991, n. 4710).
Ai fini della individuazione delle misure idonee un aiuto può venire dallo standard BS 7799 e lo standard ISO 17799 che lo ha adottato
Lo standard ISO 17799 si struttura come l'ISO9000 per le certificazioni di qualità.
Lo standard si sviluppa attraverso due elementi:

- **La politica di sicurezza**
- **Il sistema di governo della sicurezza dell'informazione**

La politica di sicurezza costituisce l'insieme degli obiettivi di sicurezza dei dati personali che si intende adottare in funzione della loro tutela.
Il sistema di governo della sicurezza dell'informazione è l'insieme dei meccanismi di sicurezza adottati ed aggiornati al fine di mantenere il livello di protezione dei dati sempre costante nel tempo.
Lo standard BS 7799 ha individuato il seguente modello di sistema di governo della sicurezza dell'informazione dinamico laddove le scelte effettuate vengono sempre rivisitate ed implementate nel tempo per conservare il livello di sicurezza e protezione dei dati conformemente agli sviluppi tecnologici.

Modello di sistema di governo della sicurezza dell'informazione adottato dallo standard BS7799

Lo stesso standard individua anche un elenco di attività di controllo ed esecutive da rispettare per garantire la sicurezza dei dati personali.

Parte di tali attività sono state recepite dal legislatore della Privacy nell'Allegato B) al Codice della Privacy.

MISURE MINIME

Nell'affrontare il tema delle misure minime è opportuno l'analisi distinta tra

- **il trattamento effettuato con l'uso di strumenti elettronici**
- **il trattamento effettuato senza l'uso di tali strumenti.**

La distinzione è doverosa per le diverse implicazioni determinate dalla scelta di trattamento attraverso l'una o l'altra modalità.

Trattamento effettuato con l'uso di strumenti elettronici

Tale ipotesi è affrontata dal legislatore della Privacy nell'art. 34 del Codice e nel Disciplinare Tecnico contenuto nell'Allegato B) del Codice.
Tra le novità che possono individuarsi nell'attuale normativa è la scomparsa del termine elaboratore elettronico usato nel precedente D.P.R. e la eliminazione della distinzione tra pc stand alone e pc collegato in rete.
Il Codice della Privacy fa riferimento al più generico concetto di strumento elettronico laddove per tale può intendersi qualsiasi strumenti idoneo a conservare dati personali quale una smart-card, un telefono cellulare con una scheda di memoria versatile, una macchina fotografica digitale, una penna memory stick e quant'altro sia suscettibile di acquisire e conservare dati personali.
Ulteriore novità è la scomparsa della figura dell'Amministratore di sistema definito dal D.P.R. 318/99 come colui al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. Tale figura, pur se formalmente scomparsa, è fondamentale per il preciso funzionamento degli strumenti elettronici usati all'interno dello Studio e per consentire di adottare tutte quelle iniziative volte al buon funzionamento dell'hardware e del software usato.
E' vivamente consigliato evitare un uso promiscuo dello strumento elettronico usato nello Studio Legale per il trattamento dei dati. Pertanto sarebbe opportuno che il pc dedicato al lavoro dello Studio ed al trattamento dei dati non sia utilizzato per una connessione ad internet per usi privati (chat, scaricamento di programmi di diletto, collegamento a server di scambio file, ecc) ovvero per provare programmi nuovi, ovvero per ragioni non direttamente connessi con l'esercizio dell'attività.
Le misure minime sono individuate nell'art. 34 del Codice della Privacy sotto forma di elenco e con un rimando,quanto alle modalità applicative, al Disciplinare Tecnico contenuto nell'Allegato B)

a) Autenticazione informatica

Il legislatore del 2003 ha usato correttamente il termine autenticazione informatica in luogo di autorizzazione di accesso usata nel D.P.R. 318/99
Infatti, l'autorizzazione di accesso ai dati presuppone l'avvenuta individuazione corretta del soggetto autorizzato ad accedere ai dati.
Il legislatore del 2003 si è preoccupato di disciplinare l'identificazione precisa del soggetto autorizzato attraverso una serie di elementi.
Infatti, il sistema di autenticazione è proteso ad individuare con precisione chi intende accedere ai dati personali contenuti in un sistema informatico.
Forse sarebbe stato più opportuno usare l'espressione " verifica dell'identità dell'utente"
D'altronde un sistema di verifica dell'identità del soggetto autorizzato ad accedere ai dati consente da un lato di controllare chi accede ai dati e dall'altro di attribuire la responsabilità ad un soggetto specifico per gli eventuali usi impropri dei dati.
L'autenticazione informatica si sviluppa attraverso l'accertamento di due elementi:

- **il codice di identificazione**
- **il codice di verifica dell'identità**

Codice di identificazione
Il codice di identificazione consiste nell'attribuzione di un nome ad ogni utente.
Nella tecnica informatica tale codice viene chiamato solitamente *User Id*
In genere il codice di identificazione corrisponde al nome del soggetto che opera ovvero al suo numero di matricola.
In uno Studio di piccole dimensioni lo User Id può identificarsi con lo strumento elettronico ad esempio " Segreteria", "Praticante", "Avvocato" o altro. Di solito negli studi di piccole dimensioni si è solito usare tale tipo di codice di identificazione perché più comodo ed anche perché solitamente un certo pc viene usato sempre dalla stessa persona.
Il punto 6 del Disciplinare Tecnico precisa che il codice di identificazione è personale solo laddove utilizzato; ciò lascerebbe intendere che il codice di identificazione potrebbe essere unico per postazione; tuttavia non sempre il rispetto letterale del punto 6 del Disciplinare Tecnico potrebbe soddisfare la ratio normativa. Infatti, solo un codice identificativo personale consentirebbe a posteriore di individuare il soggetto che ha avuto accesso ai dati in un certo momento anche al fine di individuare chi può avere messo fuori uso il pc ovvero chi ha compiuto operazioni irregolare sul trattamento dei dati.

Codice di verifica dell'identità.
Il Codice di verifica dell'identità consiste nel superamento della prova di accertamento della identità del soggetto attraverso il riscontro della corrispondenza del soggetto autorizzato con il codice di identificazione con chi materialmente sta accedendo ai dati personali.
Nell'attuale panorama di conoscenze tecniche si possono individuare tre tipi di codice di verifica dell'identità:

- **una parola chiave o *password* che consiste in una informazione nota solo all'operatore;**
- **un oggetto posseduto in via esclusiva dall'operatore;**
- **una caratteristica fisica personale dell'operatore.**

Parola chiave o Password
Il tipo più comune di verifica dell'identità è la ***password***.
Per quanto criticato, perché facilmente eludibile, l'uso di tale sistema di verifica è sufficientemente sicuro. Infatti, il Governo Federale degli Stati Uniti lo ha usato per molti anni
La parola chiave è una composizione alfanumerica la cui lunghezza è fissata al punto 5 del Disciplinare Tecnico nella misura di almeno 8 caratteri ovvero se il sistema non lo consente, nel numero massimo di caratteri consentito.
Il Disciplinare Tecnico non indica se la parola chiave debba essere composta solo da numeri o solo da parole.
Nella scelta della parola chiave è preferibile una composizione alfanumerica. Infatti, il numero di parole che possono comporsi in una stringa di 8 caratteri utilizzando una composizione mista di parole e numeri è maggiore di una composizione di soli numeri o lettere della stessa lunghezza.
Nella scelta della parola chiave il Disciplinare Tecnico ha precisato che la stessa non deve avere riferimenti che possano ricondurla all'utente quale il suo cognome, nome, data di nascita, il nome di suoi figli, della moglie, luogo di nascita ecc.
Pertanto la *password* non deve essere così banale da consentire a chiunque di scoprirla, tuttavia la scelta dalla parola chiave deve corrispondere a criteri che consentano all'utente di operare sullo strumento elettronico.
Pertanto la *password* deve corrispondere ai seguenti requisiti:

- **facilmente individuata dall'utente;**
- **ricordata con facilità**
- **digitata senza difficoltà.**

Ogni utente potrà utilizzare la tecnica che ritiene più opportuna per elaborare una *password* difficilmente individuabile.
Ad esempio, una tecnica potrebbe essere quella di usare come *password* le strofe di una canzone ovvero le prime lettere delle parole di una poesia. Vi sono anche programmi generatori di *password* casuali.
Il Disciplinare Tecnico ha stabilito che la lunghezza della *password* deve essere di almeno 8 caratteri.
La ragione di una scelta siffatta riposa nelle necessità di rendere difficile la individuazione della password. Infatti, la probabilità che si possa che si possa individuare un carattere di una passowrd di 8 caratteri alfanumerici è 1 su 8^{62} e sempre che non si utilizzino caratteri speciali quali i caratteri accentati ovvero i simboli del tipo @; €; $.
Il Disciplinare Tecnico ha stabilito che la password deve essere cambiata ogni 6 mesi. Una regola ragionevole induce a ritenere più opportuno un cambiamento della password almeno ogni 3 mesi negli Studi di piccole e medie dimensioni; in quelli di maggiori dimensioni almeno ogni mese.
Il sistema informatico usato dovrebbe essere strutturato in modo tale da invitare al cambiamento della parola chiave quando si è raggiunto il tempo massimo di utilizzo della stessa. Altresì lo stesso sistema dovrebbe avere la capacità di verificare che la nuova *password* usata non sia quella usata da altro utente ovvero sia stata già usata in precedenza. Il sistema dovrebbe essere impostato in modo tale da consentire il riutilizzo di una *password* ogni *n* utilizzi
La *password* è strettamente personale ed il Disciplinare Tecnico, attento alle problematiche relative alla sicurezza delle *password*, ha adottato la tecnica della "*one time password*" consistente nell'attribuzione all'incaricato di una password che questi ha il dovere di cambiare al primo utilizzo del sistema ed il sistema deve essere strutturato in modo tale da invitare l'incaricato a cambiare la password prima dell'utilizzo del programma di accesso al trattamento dei dati personali. Una volta cambiata la password, l'incaricato dovrà riempire la scheda della password, chiuderla in una busta sigillata e consegnarla al custode delle password che se non nominato può identificarsi nel titolare del trattamento ovvero nel responsabile del trattamento.
L'attribuzione di una parola chiave personale risponde a criteri di ragionevolezza oltre che essere obbligata dal Disciplinare Tecnico, infatti, solo una *password* personale ed utilizzabile in modo esclusivo da un solo incaricato consente di individuare il responsabile in caso di uso improprio dei dati personali così come può consentire di individuare il responsabile di una cessione illecita della *password*. Infine tale criterio rende più facile la disattivazione della *password* nell'ipotesi in cui l'incaricato cessi i rapporti con lo Studio Legale.
Una parola chiave quando non è più utilizzata deve essere archiviata. L'archiviazione richiede che il sistema sia in grado di consentire l'accesso all'archivio delle *password* solo a soggetti qualificati, quali il titolare del trattamento, il responsabile del trattamento, ovvero il rappresentante del titolare, e l'amministratore di sistema se istituiti.
Altro aspetto fondamentale da tenere presente in tema di *password* è la sua digitazione.
Operativamente l'incaricato al trattamento deve poter digitare la *password* in modo da evitare che terzi estranei possano vedere la tastiera. Quanto al video tutti i più moderni sistemi prevedono che durante la digitazione della *password* non si vedano i caratteri immessi ma solo dei simboli anonimi.
Il sistema dovrà prevedere un numero massimo di tentativi di digitazione della password ovvero la disabilitazione del programma dopo un certo periodo di inattività.
Nei sistemi più complessi è prevista l'ipotesi di sblocco in caso di dimenticanza della parola chiave.
Lo sblocco potrà avvenire direttamente dall'utente attraverso un meccanismo di domanda e risposta: al momento della immissione la prima volta della *password* il sistema stabilisce con l'utente le

modalità per consentirgli di riottenere la *password* dimenticata attraverso una domanda e relativa risposta predeterminata dall'utente.
In ogni caso il titolare del trattamento ovvero il custode delle *password* devono poter accedere al sistema nell'ipotesi di blocco del sistema attraverso l'apertura della busta sigillata contenente la password ovvero attraverso una *password*-passepartout. Infatti, se l'incaricato per una ragione qualsiasi non dovesse essere al posto di lavoro, deve essere sempre possibile per il titolare accedere ai dati personali da lui trattati. Tale ipotesi è prevista dal punto 10 del Disciplinare Tecnico. L'intervento, in ipotesi di tal genere, deve avvenire nel rispetto dei diritti dell'incaricato assente; sarà necessario che l'apertura delle busta sigillata avvenga alla presenza di testimoni che attestino anche la impossibilità di accedere ai dati trattati a causa dell'assenza dell'incaricato. Dopo avere provveduto a ripristinare il sistema e l'accesso ai dati, bisognerà rendere inaccessibile al termine il pc, ripristinando la situazione al momento della prima installazione del programma di trattamento dei dati personali.
Il Disciplinare Tecnico stabilisce al punto 9 che l'incaricato al trattamento deve avere avuto istruzioni di non lasciare incustodito o accessibile il terminale o il pc e che, nell'ipotesi di certo periodo di inattività del pc, deve attivarsi un screen saver che impedisca a terzi di poter accedere ai dati ivi contenuti; per poter riattivare il pc è necessario digitare nuovamente la parola chiave.
Per gli studi di piccole-medie dimensioni possono fornirsi i seguenti suggerimenti:

1) **Si faccia coincidere la figura del Titolare del trattamento con quella del Responsabile e del Custode delle *Password*.**
2) **Si attribuisca un User Id o codice di autenticazione per ogni pc**
3) **Si attribuisca una *password* personale ad ogni incaricato, che potrà cambiarla al primo utilizzo del sistema.**
4) **Si attivi, se possibile, una *password*-passepartout**
5) **Si predisponga un registrino ove annotare le *password* e la data di attribuzione**
6) **Si custodiscano le *password* in un cassetto a chiave dopo averle sigillate.**
7) **Si predisponga uno scadenzario per il cambiamento delle *password* di tutti i pc nello stesso momento.**
8) **Si predisponga qualche accorgimento per evitare che terzi estranei allo staff dello Studio possano avere accesso alla visione del video**
9) **Si istruiscano gli incaricati di non lasciare incustoditi il pc**
10) **Si doti ogni pc di uno screen saver che riattiverà le procedure automatizzate dopo la immissione della *password*.**

Oggetto posseduto in via esclusiva dall'operatore

La verifica della identità dell'operatore potrà avvenire anche con un oggetto che possiede in via esclusiva l'utente, sia esso il Titolare, responsabile o incaricato.
In genere l'oggetto più utilizzato è un badge o scheda magnetica che viene inserita in un apposito lettore ed abilita le procedure.
Altro potrebbe essere un oggetto con apparato radio che il sistema riconosce e consente l'abilitazione delle procedure alla presenza del soggetto.
Tali sistemi non sono completamente sicuri perché facilmente duplicabili, dimenticati o persi. In tal caso non si potrebbe accedere al sistema.
Una possibile soluzione potrebbe essere quella di prevedere una scheda per l'accesso al sistema e la digitazione di una password per l'abilitazione delle procedure.

Una caratteristica fisica personale dell'operatore

Trattasi dei c.d. dispositivi di riconoscimento biometrico fondati sul riconoscimento di alcune parti del corpo del soggetto quali l'impronta digitale, la retina dell'occhio, la voce, la firma, la mano ovvero l'esame del volto.

Il Garante della Privacy non ha ritenuto che tali meccanismi di verifica del codice di identificazione siano in contrasto con la privacy dell'operatore perché tecnicamente il meccanismo di riconoscimento della caratteristica dell'operatore non si estende a tutta la parte del corpo interessata. Ad esempio, un meccanismo di verifica che si basasse sulla lettura delle impronte digitali non estenderebbe il suo esame all'intera impronta ma ad alcuni elementi che confronterebbe con quelli in suo possesso, ciò anche per la necessità di occupare poco spazio nella memoria di massa del pc dedicata a tale scopo.
In uno Studio di piccole – medie dimensioni gli ultimi due sistemi indicati di verifica del codice di identificazione non sono necessarie.
Infatti, la sicurezza delle modalità di trattamento dei dati personali in uno Studio Legale è largamente esaudita attraverso il sistema delle *password* che, peraltro ha un costo nettamente inferiore a quello necessario per dotare il sistema di un meccanismo a scheda magnetica ovvero a riconoscimento dell'impronta digitale.
L'insieme del codice di identificazione e di quello di verifica costituiscono le **credenziali di autenticazione**

b) Adozione di procedure di gestione delle credenziali di autenticazione

Il Disciplinare Tecnico ai punti da 7 a 10 fornisce indicazioni sulle modalità di gestione delle credenziali di autenticazione.
Le credenziali di autenticazioni non utilizzate per almeno sei mesi devono essere disattivate salvo quelle relative alle necessità di gestione tecnica (c.d. user-id e *password*-passepartout)
Il sistema potrà prevedere l'automatica disattivazione in caso di non utilizzo della *password*
Le credenziali di autenticazione vanno ovviamente disattivate nel momento in cui l'incaricato del trattamento non faccia più parte dello Studio.
Rientrano tra le procedure di gestioni anche le istruzioni sulle modalità di uso del pc da parte dell'incaricato delle quali si è già parlato nella pagina precedente.

c) Utilizzazione di un sistema di autorizzazione

Non è sufficiente prevedere un meccanismo di accertamento delle credenziali di autenticazione per rendere sicuro il sistema di trattamento dei dati personali.
E' altresì necessario prevedere un meccanismo di individuazione dei criteri di accesso ai dati personali per il loro trattamento attraverso un sistema di autorizzazione.
Si può definire Sistema di Autorizzazione il complesso degli strumenti elettronici e delle modalità di abilitazione all'accesso e trattamento dei dati in relazione a ciascun Profilo di Autorizzazione previsto per ogni utente.
Per Profilo di Autorizzazione può definirsi il complesso degli elementi abbinati univocamente ad un soggetto che consenta di individuare a quali dati egli può accedere e quali trattamenti può effettuare.
In parole povere con un sistema di autorizzazione si individua "*Chi"* può fare "*Cosa*"
In uno Studio Legale non sempre tutti i componenti hanno gli stessi compiti; né il Titolare del trattamento ha interesse a consentire l'accesso a chiunque su tutti i dati.
Pertanto bisognerà individuare un Profilo di Autorizzazione personalizzato per ogni singolo operatore, sia esso Titolare, Responsabile o Incaricato.
Nella strutturazione di un Profilo di Autorizzazione dovrà predisporsi un mansionario che stabilisca a quali risorse ogni utente avrà accesso e con quali modalità potrà accedervi.
Uno schema di sistema di autorizzazione potrà essere così strutturato:

Titolare e/o Responsabile : accesso a tutti i dati.
Responsabile del Sistema: accesso a tutti i dati.
Custode delle *password*: accesso ai dati in funzione delle sue mansioni.
Segreteria : l'incaricato addetto potrà avere accesso ai dati personali ma non a quelli sensibili; in particolare potrà stabilirsi che l'incaricato addetto occupandosi della gestione contabile dello Studio potrà avere accesso

ai dati dei clienti e dei terzi in funzione della gestione contabile. Altrettanto dicasi per la gestione degli appuntamenti: la Segreteria potrà avere accesso ai dati personali dei terzi in funzione degli adempimenti di udienza e conseguenti per la gestione degli appuntamenti, degli adempimenti e delle scadenze. L'incaricato addetto potrà avere accesso ai dati archiviati solo se strettamente necessario alle funzioni assegnate

Praticanti: accesso alle cartelle e file di elaborazione documenti contenenti anche i dati sensibili purchè per questi ultimi vi sia controllo di uso non ripetuto. All'uopo potrà predisporsi che il Titolare abiliti l'accesso di volta in volta. Il praticante potrà avere accesso ai dati archiviati solo sotto stretto controllo del Titolare o del Responsabile.

Il Sistema di Autorizzazione dovrà essere predisposto all'inizio del trattamento per ciascun incaricato

Il Disciplinare Tecnico prevede al punto 14 che periodicamente ed almeno ogni anno sia verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, pertanto una modifica delle mansioni comporterà la modifica del Profilo di Autorizzazione.

Da un punto di vista tecnico dovranno strutturarsi le password in modo tale che chi è autorizzato ad accedere e trattare dati personali non possa accedere agli altri dati. Ad esempio, l'addetto alla Segreteria non potrà accedere ai file dei documenti se non è previsto che egli possa utilizzare le procedure di formazione degli atti e dei documenti.

Infine un Sistema di Autorizzazione potrà prevedere i livelli di accesso temporale in modo da escludere che alcuni soggetti possano accedere e trattare i dati in orari diversi da quelli c.d. d'ufficio

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.

In uno Studio Legale la prima parte di tale adempimento può ritenersi soddisfatta attraverso gli adempimenti previsti dal punto 14 del Disciplinare Tecnico come sopra specificato.

Diversa è la figura dell'addetto alla gestione o alla manutenzione degli strumenti elettronici.

L'individuazione di tale soggetto è fondamentale perché il punto 23 del Disciplinare Tecnico sancisce l'obbligo di ripristino degli strumenti elettronici entro 7 giorni dal loro danneggiamento; ciò anche in funzione di rendere operativo l'obbligo di riscontrare alle richieste dell'interessato senza ritardo, giusta quanto indicato dall'art. 8 del Codice della Privacy.

La scelta deve ricadere su un soggetto esperto poiché l'addetto alla manutenzione deve intervenire senza indugio sia sull'hardware che sul software.

L'addetto alla manutenzione non solo deve conoscere il funzionamento del programma applicativo ma deve essere in grado di intervenire sul sistema operativo; sui software di sicurezza anti intrusione ed antivirus oltre che sull'hardware.

Se all'interno dello Studio non vi è una persona particolarmente esperta che sia in grado di assumere tale ruolo, è opportuno stipulare un contratto di assistenza e manutenzione con un professionista del settore.

Nel contratto di assistenza si dovrà prevedere l'obbligo di intervento immediato, ovvero in modo da garantire il ripristino della funzionalità completa del sistema entro 7 giorni. Altresì il contratto dovrà prevedere che nell'ipotesi di trasferimento dell'hardware presso la sede dell'esperto, i dati contenuti nella memoria di massa dell'hardware non siano dallo stesso utilizzati, visionati e comunque trattati in alcun modo, fissando una penale nel caso di inosservanza a tale obbligo ovvero all'obbligo di ripristino entro 7 giorni.

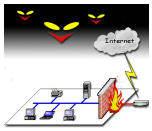
e) Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

Il Disciplinare Tecnico ai punti 16, 17 e dal 20 al detta regole per rendere operativa tale prescrizione.
Il Punto 16 del Disciplinare Tecnico stabilisce l'obbligo di protezione dei dati dal rischio di intrusione e dei programmi di cui all'art. 615 quinquies c.p. attraverso l'attivazione di idonei strumenti elettronici da aggiornare almeno ogni sei mesi
Il Punto 17 invece impone l'obbligo di aggiornare almeno una volta l'anno i programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e correggerne eventuali difetti salvo che non vengano trattati dati sensibili allorché l'aggiornamento deve avvenire almeno ogni sei mesi.
Una lettura superficiale del Disciplinare Tecnico potrebbe indurre a ritenere soddisfatto l'obbligo di legge con l'acquisto o l'installazione di un antivirus e di aggiornarlo periodicamente.
Invero il legislatore della Privacy, attento alle evoluzioni tecnologiche, ha usato il termine di intrusione e vulnerabilità del sistema che ovviamente ha ben altro significato di un semplice attacco di un virus.
Appare opportuno affrontare in questa sede l'argomento della sicurezza informatica che costituisce l'antecedente logico e pratico alla sicurezza dei dati.
Allorquando il legislatore ha usato la terminologia di tecniche di intrusione si è voluto riferire ai pericoli per la sicurezza dei dati che possono provenire dal collegamento del pc ad internet
Le tecniche di intrusione con il passare degli anni si sono fatte sempre più pericolose e più subdole, perciò il virus rientra nella più estesa categoria dei software maligni denominati nella comune accezione ***malware***
I malware possono distinguersi in quelli diretti a danneggiare il sistema compromettendone il regolare funzionamento e provocando il danneggiamento dei dati ivi contenuti ed in quelli che, invadendo il sistema, violano la privacy dell'utente.
Tra i primi si annoverano i virus intesi come programmi che si moltiplicano attraverso la diffusione in rete ed attraverso i quali i file contenuti nell'hard disk vengono cancellati. Il pericolo delle nuove forme di virus, come il famoso *I Love You*, è rappresentato dalla rapidità della loro diffusione, perché, in genere, questi nuovi virus contengono istruzioni per replicarsi e per trasmettersi a tutti i contatti contenuti nel programma di posta elettronica, con la conseguenza che tutti i contatti ricevono un messaggio di posta elettronica contenente come allegato il file infettato.
La forma più recente di virus conosciuta è il ***worm*** (verme) perché non solo è autoreplicante ma è in grado di attivarsi anche senza l'intervento umano, sfruttando i bug del sistema. A tal proposito Microsoft provvede periodicamente a mettere in rete una *patch* (pezza) diretta ad eliminare i bug del sistema.
Un altro tipo di malware particolarmente pericoloso è il ***trojan***.
Tale tipo di malware che prende il nome dal cavallo di Troia, consiste in un programmino contenuto all'interno di un altro programma o di un altro file che esegue regolarmente la sua funzione, ma che alla sua prima apertura attiva il trojan. Una volta attivato, il trojan si insedia nel sistema operativo e si attiva ogni volta che il pc viene acceso. Attraverso questo programma il pc infettato e collegato ad internet si trasforma in un server al quale un altro pc ,anch'esso collegato in internet, con un programma di collegamento con il trojan, accede liberamente. In buona sostanza ogni qualvolta ci si collega ad internet con un pc infetto da un trojan, il *cracker* che ha infettato il pc, automaticamente può accedere, controllare, manipolare,cancellare tutto o parte del contenuto dell'hard disk oltre che immettere dati e file nel pc infetto e fare attivare altri e nuovi programmi, Si è preferito usare il termine corretto di *cracker* al posto di quello più comunemente conosciuto come hacker perché quest'ultimo è un programmatore esperto dei sistemi operativi e delle problematiche connesse alla violazione del sistema ed il cracker è colui che viola i sistemi informatici in modo e per motivi illeciti. Tuttavia il *cracker* può accedere ad un pc ed infettarlo con un trojan anche senza l'apertura di un file, sfruttando le vulnerabilità della rete e la vulnerabilità delle porte di accesso ad internet del

pc. In poche parole il *cracker* con un programma denominato *portscan* verifica se il pc interessato abbia una porta di connessione *non sorvegliata* e sferra l'attacco introducendosi nel pc
Infine ci sono i virus c.d. buoni che si preoccupano di individuare il malware e di rimuoverlo. Spesso, però, il *cracker* usa mascherare il malware da virus buono.
Tra i secondi si annoverano gli *spyware* che hanno la funzione di spiare i comportamenti dell'utente connesso ad internet ed inviare informazioni relative a comportamenti o al sistema del pc collegato a qualcuno che può utilizzarle per inviare posta indesiderata (c.d. spam) ovvero per scopi illeciti; gli adware che hanno la funzione di aprire fastidiosissime finestre pubblicitarie durante la navigazione in internet; il dialer che è costituito da un programma che promettendo l'accesso a siti per adulti in modo "gratuito", ovvero a siti dai quali è possibile scaricare suonerie o programmi "gratuiti, una volta attivato disconnette il modem dalla linea telefonica cui è connesso e lo collega ad un numero a pagamento quale il 144, 166 ecc.
Una delle forme di diffusione dei virus avviene attraverso messaggi di posta elettronica.
Una buona regola è quella di non aprire mai un allegato di posta elettronica se proviene da un mittente sconosciuto.
Tuttavia anche nell'ipotesi in cui un allegato di posta proviene da una persona a noi nota, è sempre meglio accertarsi se il mittente abbia effettivamente spedito il messaggi di posta con l'allegato.
Infatti l'invio di fake e-mail (falsa e-mail) è una tecnica di trasmissione di posta elettronica con allegato infetto. E' abbastanza facile anche senza la conoscenza di particolari tecniche informatiche inviare una fake e mail, mediante la modifica dell'account di posta elettronica. In sostanza, quando si imposta un indirizzo di posta elettronica nel programma di posta elettronica si forniscono indicazioni nel pannello generale dell'account. La modifica di queste consente di spedire posta elettronica sotto falso nome.
Orbene al momento del ricevimento del messaggio, se l'utente è registrato nei contatti il programma indicherà il mittente con il nome indicato nell'account modificato. In questo caso l'utente ritenendo di potersi fidare del messaggio ricevuto aprirà l'allegato e così inconsapevolmente avrà attivato il virus.
E' vivamente consigliato non aprire mai allegati di posta elettronica che siano dei file eseguibili. I file eseguibili sono quelli che contengono programmi; tecnicamente sono quelli che hanno una estensione *.exe*
Tuttavia una tecnica usata dal *cracker* è quella di modificare l'estensione del file attribuendogli una estensione più tranquilla ad esempio *.doc* (file documento di word) ovvero . *jpg* (file immagine); a volte l'allegato ha una doppia estensione confidando nel fatto che, in genere, nel sistema operativo Windows nel pannello *Visualizzazione di Opzione Cartelle* vi è l'opzione di spunta nel pannello *nascondi estensione per i tipi di file conosciuti*. Pertanto allorquando si riceve un file di posta elettronica la visualizzazione dell'allegato indica che trattasi di file innocuo ma ciò non è.
E' bene precisare che nell'ipotesi di una fake e mail *potrebbe* essere possibile risalire al mittente originale attraverso la verifica dei dettagli del messaggio dalle proprietà del messaggio. In tale riquadro potrà individuarsi da quale server e con quale IP il mittente ha inviato il messaggio, laddove per IP si intende l'Identificativo Personale attribuito dal server all'utente connesso ad internet. Conseguentemente attraverso una denuncia all'Autorità Giudiziaria potranno attivarsi le indagini per l'individuazione del soggetto che ha inviato il messaggio con allegato infetto.
Si è usato il termine condizionale *potrebbe* perché in realtà il messaggio potrebbe essere inviato attraverso un indirizzo IP diverso con una tecnica chiamata IP Spoofing, che consente di camuffare l'IP e di inviare e-mail in modo anonimo ovvero attraverso l'uso di un pc infettato che diventa uno "zombie" agli ordini del *cracker* che lo userà per inviare e-mail a terzi che riterranno di ricevere i messaggi di posta dall'ignara vittima.
Da qualche tempo, stanno arrivando messaggi di posta elettronica con il logo Microsoft che invita l'utente ad aprire un allegato al messaggio costituente una patch di aggiornamento per prevenire attacchi da virus: ebbene trattasi di una e-mail contenente un virus. **Non aprite assolutamente l'allegato**! Infatti, è del tutto inimmaginabile che la Microsoft utilizzi la posta elettronica per

inviare gli aggiornamenti del sistema operativo; men che mai qualcuno potrà avere la pretesa di ritenersi così conosciuto alla Microsoft per ottenere il privilegio di un aggiornamento personalizzato del sistema operativo.
Infine una ulteriore fonte di intrusione è l'uso di programmi di scambio file comunemente chiamati file sharing attraverso una connessione P2P. Il file sharing è usato per lo scambio di file audiovisivi o musicali. Per poter accedere a tale tipo di scambio è necessario utilizzare un programma denominato P2P che consente ad ogni utente di condividere una cartella per lo scambio, così facendo si consente di tenere aperta una porta che un malintenzionato potrebbe usare per accedere al pc.
Come proteggersi dai malware?
Il Disciplinare Tecnico impone l'obbligo di dotare il sistema informatico di un antivirus al quale far scansionare tutti i file ivi compresi quelli ricevuti via e mail cancellando quelli infetti.

Il Sans Institute cui fanno parte esperti del settore ha redatto una linea guida per prevenire possibili attacchi da virus.
Al fine di evitare attacchi intrusivi derivanti da programmi quali portscan è bene dotarsi di un firewall (muro di fuoco) che è un programma che frapponendosi tra il modem ed il pc collegato ad internet, blocca tutti i potenziali attacchi che provengono dalla rete.



Un buon antivirus e firewall dovrebbe avere le seguenti caratteristiche alcune delle quali sono, tra l'altro, richieste dal Disciplinare Tecnico di cui all'Allegato B) del Codice della Privacy:

- **idoneità di effettuare una scansione del pc al momento della sua accensione analizzando i file di boot e system;**
- **essere sempre attivo durante il collegamento ad internet;**
- **scansionare la messaggistica di posta elettronica ed i suoi allegati prima e durante lo scarico sul pc;**
- **bloccare le intrusioni provenienti da programmi, documenti e comunque istruzioni contenute nei file ricevuti ovvero nei file che tentano di introdursi indebitamente nel pc attraverso porte libere;**
- **cancellare i file infetti ovvero, nel caso non sia possibile, riporli in quarantena;**
- **essere aggiornabile via internet ovvero in altro modo e prevedere un meccanismo di allarme per l'aggiornamento; ovviamente l'aggiornamento dovrà riguardare non solo la definizione dei virus ma anche quello del programma antivirus o firewall**

Il Disciplinare Tecnico ha previsto una forma di aggiornamento di tali programmi almeno semestrale. E' vivamente consigliato aggiornare i programmi (non solo la definizione dei virus) con cadenza settimanale o quindicinale; infatti, un aggiornamento con periodicità maggiore costituisce adozione di misura idonea.
E' altresì vivamente consigliata la verifica del periodo di validità dell'abbonamento al programma. Infatti, se l'abbonamento è scaduto il programma di solito consente al massimo l'aggiornamento delle definizioni dei virus.
In commercio esistono dei programmi integrati che contengono sia un antivirus che un firewall (ad esempio il Norton Internet Security).
Tuttavia in commercio vi sono antivirus e firewall gratuiti. (Nel cd allegato sono inclusi due antivirus, un Firewall ed altri programmi di utilità)
Una nuova minaccia informatica sta rapidamente diffondendosi: *il phishing*.

Il nome trae origine dal termine inglese *fishing* (pescare): il malintenzionato pesca nella rete ignare vittime
Trattasi di una truffa ben architettata attraverso artifici e raggiri che inducendo in errore l'utente contattato consente al malintenzionato di ottenere informazioni riservate quali lo *user id* (il nome utente) e la *password* per l'accesso a sezioni riservate per l'utente di siti istituzionali, di banche, di banche dati in abbonamento, di commercio elettronico o altro.
Il truffatore invia una e mail ad una serie indefinita di utenti nella quale, utilizzando i loghi, per esempio di una banca, paventando la necessità della verifica dei dati personali dell'utente per i più svariati motivi (manutenzione del server o altro). In calce all'e mail viene indicato un indirizzo web al quale connettersi. L'utente connettendosi all'indirizzo indicato vedrà aprirsi una finestra con i loghi del sito della sua banca ovvero, addirittura una *home page* del tutto simile a quella originale del sito della banca. L'utente provvederà a *loggarsi* nella sezione riservata immettendo il proprio *user id* e la propria *password*. L'utente non accederà a nessuna sezione del sito ma si ritroverà di nuovo nella *home page* (questa volta quella reale) della banca e penserà che per motivi di connessione non è riuscito a connettersi e riproverà verificando la correttezza dei suoi dati. L'utente riterrà di non avere necessità di effettuare cambiamenti e chiuderà la finestra del *browser*. I dati dell'ignaro utente, nel frattempo, sono stati trasmessi al truffatore che potrà utilizzarli accedendo alla banca per effettuare operazioni illecite sul conto corrente del malcapitato. Ci si può accorgere della truffa verificando il nome dell'indirizzo web che di solito è contrassegnato da una serie di numeri (indirizzo IP) e che normalmente una banca non indica. Da ultimo è stata scoperta una più raffinata tecnica denominata *pharming* attraverso la quale il truffatore sfruttando alcune vulnerabilità della rete utilizza il sito ufficiale della banca per effettuare un reindirizzamento ad un altro sito creato appositamente per perpretare la truffa. E' vivamente consigliato di ignorare messaggi che provengano da banche o altre istituzioni private o pubbliche che invitano l'utente a verifiche dei propri dati; se si hanno dubbi è consigliabile contattare direttamente l'ufficio istituzionale del soggetto che ci ha inviato l'*e mail* per la verifica dell'autenticità del messaggio ricevuto
Infine è opportuno evidenziare che, sebbene si possa avere adottato la misura di sicurezza informatica più efficace, rimane sempre un anello debole nella catena della sicurezza informatica: l**'uomo**
Il dott. Costabile Gerardo, membro dell'International Association of Computer Investigative Specialists, nel corso dei suoi innumerevoli interventi in tutta Italia, ha avuto modo di spiegare che uno dei maggiori pericoli per la sicurezza informatica viene dall'attività dei c.d. ingegneri sociali, persone che attraverso il telefono riescono ad ottenere dati ed informazioni per poter violare i sistemi attraverso una tecnica chiamata di social engineering. Il c.d. ingegnere sociale è colui che con tecniche di persuasione, riesce ad ottenere informazioni riservate, ad esempio, qualificandosi come ufficiale di P.G. potrebbe ottenere informazioni riservate su alcuni fascicoli dello Studio, ovvero qualificandosi come tecnico della Telecom ottenere password di accesso ai sistemi per una paventata necessità di controllo delle procedure di accesso ad internet.
Buona regola è quella di verificare sempre la provenienza delle richieste di informazioni per via telefonica e fornirle solo se strettamente necessario.

f) Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Il Disciplinare Tecnico al punto 18 molto più semplicemente sancisce l'obbligo di *impartire istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con cadenza almeno settimanale.*
Il legislatore ha usato un termine estremamente generico (*salvataggio*) che lascerebbe intendere al lettore più ingenuo la sufficienza di salvataggio dei dati in un archivio cartaceo. Invero il legislatore ha inteso riferirsi a quello che in senso tecnico si chiama *backup* dei dati

Il backup è di intuitiva importanza specie per chi solitamente usa un pc con sistema windows collegato alla rete internet.
Infatti, molto spesso accade che il pc vada in panne anche per un errore prodottosi nel sistema operativo a causa dell'installazione di un programma che va in conflitto con la struttura del sistema operativo usato nel pc (il sistema operativo può avere delle conformazioni diverse a seconda dei programmi che vengono installati che vanno ad incidere su parti di esso: le c.d. librerie).
Creare delle copie di backup costituisce non solo rispetto dell'obbligo di adozione delle misure minime ma anche quello di adozione delle misure idonee.
Nella predisporre l'organizzazione delle procedure di backup bisognerà tener conto di operazioni da eseguirsi tra le quali possono suggerirsi le seguenti:

- **individuazione del soggetto deputato alle operazioni di backup;**
- **individuazione dei dati da archiviare;**
- **scelta del supporto di archiviazione;**
- **fissazione della regola del cambiamento periodico dei supporti di archiviazione;**
- **etichettatura in modo sicuro dei supporti di archiviazione;**
- **individuazione di un luogo di conservazione dei dati di backup;**
- **individuazione di ogni eventuale procedura per evitare che quanto archiviato nei supporti possa essere smarrito, danneggiato ovvero reso inutilizzabile;**
- **scelta della modalità di archiviazione;**
- **verifica della integrità di quanto verrà archiviato prima della sua archiviazione.**

E vivamente consigliato avere delle copie di rispetto non solo dei dati ma anche dei programmi e del sistema operativo. E' opportuno evidenziare che ogni contratto di licenza software consente una o più copie del programma ai fini di operazioni di ripristino.
Pertanto è opportuno che tutti i programmi originali e le copie di rispetto, opportunamente contrassegnate, siano conservate in luogo riservato e in modo tale da poter essere recuperate con facilità al bisogno.
Quanto all'archiviazione dei dati si suggerisce di avere una concezione più ampia di dato rispetto a quello cui si riferisce il Codice della Privacy. Infatti sarebbe opportuno prevedere l'archiviazione periodica, non solo dei dati personali che vengono trattati nello Studio Legale ma, di tutti i dati, file o documento necessari per l'esercizio dell'attività professionale. Ad esempio per chi dovesse utilizzare un foglio elettronico per la gestione del Giornale del Fallimento è opportuno fare copie di salvataggio dei relativi file per non dover procedere alla rielaborazione della contabilità nell'ipotesi di perdita del relativo file. Per i file di documento (foglio di calcolo; documento; database ecc.) si consiglia di salvare il documento con un nuovo nome in modo di averne un clone. Infatti, nell'ipotesi di danneggiamento del file sarà possibile recuperare il suo contenuto dal clone.
Sarebbe opportuno che il soggetto deputato alle operazioni di backup sia sempre lo stesso per evitare pericolo di dimenticanze e confusioni.
I supporti di archiviazione possono essere diversi; può utilizzarsi una specifica macchina in rete che funga da server su cui archiviare tutti i dati.Alcune di queste macchine più evolute sono dotate di più dischi fissi (hard disk) che, collegati tra loro ed utilizzando una particolare procedura, effettuano una copia dei dati su tutti i dischi in modo da consentire una maggiore sicurezza in caso di danneggiamento di uno dei dischi . Se si sceglie tale soluzione è opportuno che tale macchina sia isolata dal collegamento ad una rete internet. Altri supporti di archiviazione possono essere i floppy disk; dischi removibili; cd; dvd; cartucce ecc. Il sistema più economico è l'uso di cd riscrivibili ovvero l'uso di dischi removibili per la maggiore capacità di conservazione che altri sistemi non hanno.
I supporti di archiviazione devono essere etichettati preferibilmente in modo chiaro per evitare che possano essere confusi con altri supporti.
Ci sono diversi tipi di modalità di archiviazione:

copia integrale	è la copia completa di tutti i dati; richiede un maggiore tempo di archiviazione e si estende anche ai dati non modificati
copia incrementale	è la copia in nuovo file solo di quelli nuovi e/o modificati rispetto alla copia precedente; i tempi di archiviazione si riducono ma potrebbe essere necessario ricostruire gli archivi attraverso la ricostruzione di tutti i file incrementati
copia differenziale	è la copia in nuovo file dei soli file nuovi e/o modificati rispetto all'ultima copia completa; richiede un minore tempo di archiviazione ed un minor tempo di archiviazione essendo sufficiente per la ricostruzione usare la copia completa e l'ultima copia differenziata.

Sebbene la copia integrale richieda un tempo maggiore di archiviazione è ritenuta più sicura e comoda, perché necessita di un minor numero di supporti di archiviazione e un minor tempo per la ricostruzione.
I supporti di archiviazione vanno conservati in luogo sicuro e vanno tenuti lontano da fonti di calore e da fonti magnetiche per evitare che possano deteriorarsi fisicamente ovvero smagnetizzarsi. Nell'una e nell'altra ipotesi la ricostruzione potrebbe essere impossibile ovvero potrebbe essere possibile solo attraverso l'invio dei supporti a centri specializzati con tutte le conseguenza circa la riservatezza dei dati.
Il Disciplinare Tecnico dal punto 20 al 23 individua l'obbligo di istruire gli addetti circa la conservazione dei supporti di conservazione dei dati da accessi non autorizzati e trattamenti non consentiti, oltre che prevedere le operazioni di ripristino in tempi brevi.
Infine il Disciplinare Tecnico sancisce al punto 25 l'obbligo di procurarsi una dichiarazione attestante la conformità degli interventi al Disciplinare Tecnico nell'ipotesi in cui ci si avvalga di soggetti estranei allo Studio Legale per l'adozione delle misure minime di sicurezza. Esistono delle organizzazioni specifiche che si occupano di provvedere all'adozione all'interno dello Studio alla predisposizione ed adozione delle misure minime di sicurezza.

g) Tenuta di un aggiornato documento programmatico sulla sicurezza.

Il famigerato Documento Programmatico sulla Sicurezza denominato più semplicemente D.P.S. costituisce un documento che da un lato ha la funzione di fotografare l'intera struttura dello Studio sia con riferimento alle strutture fisiche che a quelle degli strumenti usati per il trattamento dei dati e, dall'altro, quella di indicare tutte le misure adottate per proteggere i dati dopo aver effettuato una valutazione dei rischi e la loro quantizzazione.
Invero una lettura comparata dell'art. 34 del Codice della Privacy con il punto 19 del Disciplinare Tecnico evidenzia una certa incongruenza; infatti, mentre per l'art. 34 il D.P.S. è una misura minima per tutti coloro che trattano dati personali, il punto 19 del Disciplinare Tecnico ne imporrebbe la redazione solo nel caso di trattamento di dati sensibili e giudiziari.
Vi è da ritenere che il legislatore abbia voluto prevedere la redazione del D.P.S. come obbligo generale per tutti i tipi di dati non prevedendo allo stato il futuro scenario dei pericoli che possano derivare dall'uso indebito anche dei dati identificativi prevedendo poi in un allegato alla legge l'obbligo imposto per i soli dati che necessitino maggiore tutela.
Tale distinzione non può riguardare gli avvocati perché trattano anche i dati sensibili e giudiziari per l'esercizio dell'attività di difesa; ne consegue la necessità della redazione del D.P.S. dagli avvocati. Infine una ragione di prudenza può giustificare la redazione del D.P.S.: consentire di offrire una prova, nell'ipotesi di denuncia ai sensi dell'art. 15 del Codice della Privacy, di avere adottato tutte le misure idonee a prevenire il verificarsi di un evento dannoso
Il D.P.S. va adottato per la prima volta entro il 31/12/2005 e successivamente va aggiornato periodicamente almeno una volta l'anno ovvero nell'ipotesi di mutamenti della situazione cristallizzata nell'ultimo D.P.S. redatto.

Il D.P.S. non ha la funzione di controllo da parte del Garante circa l'adozione delle misure di sicurezza, infatti, nell'ipotesi di controllo non verrà effettuato di certo un accertamento sulla esistenza del D.P.S. ma si verificherà se le misure minime saranno state adottate. Pertanto il D.P.S. costituisce un promemoria, legislativamente imposto, diretto ad una verifica per il titolare del trattamento di avere eseguito tutte le procedure per la salvaguardia dei dati trattati, previa valutazione dei rischi ed una loro quantizzazione.
La redazione del D.P.S. non richiede una particolare conoscenza degli aspetti tecnici ma semplicemente una attitudine alla organizzazione di una struttura sia sotto il profilo logico, sia sotto il profilo analitico, sia sotto il profilo decisionale.
Il punto 19 del Disciplinare Tecnico attribuisce al Responsabile del Trattamento, se designato, una particolare importanza imponendogli l'onere di redazione del D.P.S.
Il punto 19 del Disciplinare Tecnico detta le modalità di redazione del D.P.S. ed indica tutte le operazioni da effettuare durante la sua redazione individuando così il suo contenuto.
Preliminarmente bisognerà individuare **quali tipi di dati vengono trattati dallo Studio Legale**. Non par dubbio che qualsiasi Studio Legale tratti tutti i dati personali: identificativi; sensibili; giudiziari.
Dopo avere individuato i dati trattati bisognerà passare all'**analisi dei rischi** *di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta* (art 31 del Codice della Privacy)
Appare opportuno effettuare una elencazione dei rischi attraverso una analisi della struttura e degli strumenti in possesso dello Studio.
Il seguente elenco può costituire un esempio di indicazione dei rischi:

- **rischi di distruzione o perdita, anche accidentale dei dati;**
- **rischi di accesso non autorizzato ai dati;**
- **rischi di trattamento non consentito o non conforme alla finalità della raccolta;**
- **rischi connessi alla violazione e manipolazione dei dati;**
- **rischi connessi alla connessione in rete degli strumenti elettronici intesi sia quelli di connessione ad una rete locale che ad internet;**
- **rischi connessi all'integrità dei supporti di archiviazione e di registrazione dei dati sull'hard disk;**
- **rischi connessi alla violazione dei fascicoli di studio e dei documenti ivi contenuti;**
- **rischi connessi all'utilizzo degli archivi ove sono contenuti i fascicoli di studio;**
- **rischi connessi all'uso degli strumenti informatici;**
- **rischi di accesso non autorizzato nella struttura;**
- **rischi connessi con incendi e furti.**

A questi dovranno aggiungersi gli ulteriori rischi che si riterranno esistenti e le potenziali fonti di danno ai dati trattati.
Successivamente dovrà passarsi alla **quantizzazione dei rischi**.
La quantizzazione del rischio è una tecnica usata da molte aziende per misurare e determinare gli investimenti diretti a prevenire i danni. Nel caso in esame la quantizzazione sarà necessaria per prevenire il rischio di perdita o distruzione dei dati
Un criterio da utilizzarsi nella quantizzazione dei rischi potrà essere il seguente:

Valutazione dell'impatto e la frequenza di ogni tipo di rischio
Attribuzione di un valore ad ogni tipo di rischio
Valutazione delle misure di sicurezza da adottarsi per la prevenzione dei rischi
Individuazione:

- **delle misure che rallentano l'intrusione**
- **delle misure che segnalano l'intrusione**

- **delle misure che consentano il tempestivo intervento sul posto**

Per la quantizzazione di quanto da ultimo indicato si è soliti far ricorso alla seguente formula matematica Tp>>Ta + Ti, laddove Tp= tempo penetrazione delle difese, Ta = tempo di rilevazione intrusione e Ti = tempo di intervento.
A seguito della quantizzazione dei rischi si individuano le **misure che si intendono adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità nonché la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento dei dati trattati.**
Trattasi delle misure dirette a garantire l'efficienza della strutture e degli strumenti usati per il trattamento dei dati e delle misure di contenimento e riduzione dei danni (c.d. contingency planning) e di intervento di ripristino immediato dei dati a seguito del verificarsi di un evento accidentale di perdita degli stessi (c.d. disaster recovery).
La maggiore attenzione dovrà porsi sulle misure dirette a prevenire il verificarsi dei danni.
Infatti, qualsiasi misura di limitazione dei danni non esimerà il Titolare o il responsabile del trattamento dalle responsabilità derivategli dall'art. 15 del Codice della Privacy salva l'ipotesi di responsabilità ai sensi dell'art. 169.
Tuttavia il legislatore ha previsto l'obbligo di predisporre un piano di contenimento e riduzione dei danni e di ripristino della funzionalità del sistema per il trattamento dei dati.
Una copia dei file di sistema, dei programmi ed un backup periodico dei dati, potrà ritenersi una valida politica di contingency planning e disaster recovery.
Un'ulteriore misura da indicarsi come adottata è quella della **formazione degli incaricati** che saranno edotti sui rischi che incombono sui dati e sulle loro responsabilità e sugli obblighi loro gravanti nel trattamento dei dati. Dovrà prevedersi un ciclo di formazione periodica.
Nel D.P.S. dovrà essere indicato quale misura anche di tipo informativo sarà adottata nell'ipotesi di trasferimento all'esterno dello Studio del trattamento dei dati (ipotesi di affidamento della contabilità al commercialista dello studio; dell'affidamento di indagini difensive a investigatori privati ecc.)
Infine nel D.P.S. dovranno essere indicati i criteri per la cifratura o la separazione dei dati aventi ad oggetto lo stato di salute e la vita sessuale degli interessati.
In allegato è offerto un modello di D.P.S. che potrà essere adattato alle esigenze dello Studio Legale.
Il D.P.S. deve essere redatto entro il 31 marzo di ogni anno.
Il Codice della Privacy, per la sua prima applicazione, ha previsto come termine, per la redazione del D.P.S., il 30/06/2004, prorogato con decreto legge del 22/06/2004 al 31/12/2004, successivamente prorogato al 30/06/2005, con decreto legge del 19/11/2004 ed infine ulteriormente prorogato al 31/12/2005 con legge n. 26 del 01/03/2005.
Il D.P.S. va sottoscritto e la sottoscrizione deve essere attestata da una data certa, invero il punto 19 del Disciplinare Tecnico non prevede che la data certa della sottoscrizione del D.P.S; tuttavia l'art. 180 del Codice della Privacy stabilisce, nell'ipotesi in cui il Titolare del Trattamento, per obiettive ragioni tecniche non sia nelle condizioni di adeguare la sua struttura alle misure minime, l'obbligo di attestarne le ragioni in un atto avente data certa.
Tuti i commentatori hanno ritenuto, pertanto che la redazione del D.P.S. debba avere la data certa circa la sua redazione.
Il Garante della Privacy con un suo parere in data 05/12/2000 riferendosi alle misure minime previste dalla legge n. 325/2000 recante "Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste all'art. 15 della legge 31 dicembre 1996 n. 675" ha fornito chiarimenti, validi anche per l'attuale Codice della Privacy, sulla data certa.
In particolare, in detto parere si osserva:

In questa prospettiva, senza pretesa di indicare in modo esauriente tutti i possibili strumenti idonei ad assegnare al documento una data certa, il Garante richiama l'attenzione dei titolari del trattamento sulle seguenti possibilità che appaiono utilmente utilizzabili:

a) *ricorso alla c.d. "autoprestazione" presso uffici postali prevista dall'art. 8 del d.lg. 22 luglio 1999, n. 261, con apposizione del timbro direttamente sul documento avente corpo unico, anziché sull'involucro che lo contiene;*
b) *in particolare per le amministrazioni pubbliche, adozione di un atto deliberativo di cui sia certa la data in base alla disciplina della formazione, numerazione e pubblicazione dell'atto;*
c) *apposizione della c.d. marca temporale sui documenti informatici (art. 15, comma 2, legge 15 marzo 1997, n. 59; d.P.R. 10 novembre 1997, n. 513; artt. 52 ss. d.P.C.M. 8 febbraio 1999);*
d) *apposizione di autentica, deposito del documento o vidimazione di un verbale, in conformità alla legge notarile; formazione di un atto pubblico;*
e) *registrazione o produzione del documento a norma di legge presso un ufficio pubblico.*

Si suggerisce anche il ricorso alla sottoscrizione autenticata dal Cancelliere

Cancellazione dei dati sensibili contenuti nei supporti removibili

Il Punto 22 del Disciplinare Tecnico prevede la cancellazione dei dati sensibili, se non utilizzati, dai supporti removibili ovvero resi indisponibili a chiunque.
Il tema della cancellazione dei dati richiede particolare attenzione da parte dell'utente. Infatti, non è sufficiente cancellare un dato attraverso la normale procedura prevista dal sistema operativo. Vi sono programmi in grado di recuperare dati anche da un supporto apparentemente vuoto e persino formattato e sistemi in grado di recuperare dati da un supporto fisicamente danneggiato.
Sistemi per la cancellazione dei dati sufficientemente sicuri sono: la smagnetizzazione del supporto che, però, richiede apposita attrezzatura; la riscrittura del supporto con file di nessun rilievo fino al suo completo riempimento seguita da una nuova eliminazione dei file; l'uso di programmi specifici per la cancellazione definitiva dei dati.

Trattamento effettuato senza l'uso di strumenti elettronici

Tale ipotesi è affrontata dal legislatore della Privacy nell'art. 35 del Codice e nel Disciplinare Tecnico contenuto nell'Allegato B) del Codice.
Gli accorgimenti da adottare in tale ipotesi sono minori per l'evidente diminuzione di pericoli derivante dal mancato uso di strumenti elettronici.
In ogni caso anche nell'ipotesi di uso degli strumenti elettronici vanno adottate le misure minime di sicurezza per i dati trattati senza l'ausilio degli strumenti informatici. Infatti uno Studio Legale dotato di strumenti informatici tratta i dati anche in via cartacea e quindi soggiace anche agli obblighi previsti dalla normativa per tale trattamento.

a) **Aggiornamento periodico dell'individuazione dell'ambito di trattamento consentito ai singoli incaricati o alle unità organizzative.**
b) Previsione di procedure per una idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti.
c) Previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzate all'identificazione degli incaricati.

Il Disciplinare Tecnico ai punti 27, 28 e 29 indica le modalità tecnica da adottare in tali ipotesi stabilendo tra l'altro l'obbligo di istruzione degli incaricati circa il controllo e la custodia dei dati trattati per l'intero ciclo necessario allo svolgimento dei compiti loro affidati. Lo stesso punto fissa l'obbligo di aggiornamento delle istruzioni con cadenza annuale.
Non è opportuno distinguere le misure per tipo di dati trattati perché per l'esercizio della professione forense le regole previste per l'ipotesi più delicata è una misura idonea oltre che minima.
In primo luogo il Garante nel suo parere del 03/06/2004 ha avuto modo di precisare che non sussiste l'obbligo di oscurare la copertina dei fascicoli eliminando i nomi delle parti.
Si consiglia vivamente di redigere un mansionario nel quale siano individuati specificatamente per ogni incaricato il tipo di dati da trattare e le modalità del trattamento, ciò anche al fine di fissare i livelli di responsabilità al trattamento dei dati personali.
In uno Studio Legale di piccole-medie dimensioni tale strutturazione potrà farsi in modo flessibile stabilendo una ripartizione per classi omogenee: la Segreteria, i Collaboratori-Sostituti, i Praticanti, attribuendo a ciascuna categoria il tipo di dati da trattare e le modalità di trattamento.
Dovranno essere fissate delle regole per le modalità di utilizzo del materiale cartaceo contenente i dati personali.
In linea generale si evidenzia che tutti i fascicoli di uno Studio Legale contengono dati personali sottoposti a trattamento e, conseguentemente, necessitano di cautele e protezione da indebito uso delle informazioni ivi contenute.
I fascicoli devono essere riposti in cassettiere con chiusura a chiave ovvero riposti in una stanza separata dai luoghi di frequentazione del pubblico.
La consegna del fascicolo avverrà attraverso una indicazione da lasciare sulla cassettiera del soggetto che lo avrà prelevato, previa autorizzazione;
Di seguito si indicano a titolo esemplificativo, ma non esaustivo, alcuni accorgimenti che possono essere adottati per garantire una sicurezza dei dati:

- **individuare un luogo al riparo da un facile accesso di terzi estranei che possa contenere in modo sicuro gli archivi (le cassettiere, o altri sistemi di raccolta e conservazione dei fascicoli di studio);**
- **stabilire che l'incaricato possa prelevare solo un fascicolo per volta dall'archivio e tutti gli altri fascicoli necessari allo svolgimento dell'incarico ricevuto affidatogli;**
- **stabilire che il fascicolo preso dall'archivio dovrà essere utilizzato per il tempo strettamente necessario ai compiti affidati all'incaricato;**
- **stabilire che i fascicoli non potranno essere mai lasciati incustoditi sulle scrivanie;**
- **stabilire che,nell'ipotesi di ricevimento di clienti o terzi, si provveda a chiudere il fascicolo e nasconderlo alla vista del cliente per evitare che questi possa carpire informazioni sui dati personali di soggetti a lui estranei attraverso la lettura del contenuto del fascicolo lasciato involontariamente aperto;**
- **dare istruzioni di non effettuare copie fotostatiche dei documenti contenenti dati personali se non nella misura strettamente necessaria all'esercizio del mandato di difesa ricevuto;**
- **controllare che la fotocopiatrice non abbia in memoria delle copie non ancora elaborate;**
- **stabilire che le fotocopie mal riuscite non siano usate come carta da appunti e siano distrutte;**
- **stabilire che la spedizione di originali avvenga con una modalità che possa garantire la sicurezza di ricezione del documento e dei dati ivi contenuti;**
- **stabilire che tutti gli appunti, le copie dei documenti realizzati e collazionati siano distrutti dopo la stesura dell'originale;**
- **disporre la distruzione dei documenti con appositi tritadocumenti;**

- **dare istruzioni, nell'ipotesi in cui sia strettamente necessario che il fascicolo d'ufficio o i documenti ivi contenuti siano portato fuori dallo Studio per l'udienza ovvero per altri motivi, che lo stesso non non sia lasciato incustodito;**
- **stabilire che nell'ipotesi di colloqui telefonici sia vietato trattare dati personali se non per motivi strettamente connessi con l'esercizio del mandato di difesa ricevuto;**
- **stabilire che i dati personali non possono essere oggetto di divulgazione neanche per farne oggetto di esempio in corso di colloqui professionali ed extra-professionali;**
- **stabilire che l'accesso agli archivi avvenga solo negli orari di ufficio e stabilire regole per l'individuazione dei soggetti abilitati ad accedere agli archivi anche fuori degli orari di lavoro.**

Il Codice della Privacy o il Disciplinare Tecnico non indica le modalità con le quali siano impartite le istruzioni agli incaricati. Tuttavia sarebbe opportuno che apposite linee guida siano sottoposte a tutti gli incaricati nella forma di una lettera di incarico ovvero di istruzioni scritte e sottoscritte per presa visione e ricezione copia da ciascuno degli incaricati.
Infine sembra che il Codice della Privacy non preveda per questa ipotesi la redazione di un D.P.S. Tuttavia la lettura del punto 19 del Disciplinare Tecnico laddove al n. 4 prevede l'indicazione delle misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità, e laddove prevede l'obbligo di indicare le modalità di formazione degli incaricati, non consente di ritenere escluso l'obbligo della redazione del D.P.S. anche nel caso di trattamento senza l'ausilio di strumenti elettronici.

CONTROLLO DEI TERZI ABILITATI

Un ultimo aspetto riguarda il controllo degli archivi cartacei e magnetici nell'ipotesi in cui un terzo acceda nello Studio per svolgere alcune mansioni non collegate con l'attività tipica dello Studio.
Ci si riferisce alle ipotesi di accesso di conoscenti; figli o parenti in genere; ausiliari quali investigatori; addetti alle pulizie; addetti alla manutenzione dell'hardware e del software ecc.
Allorquando tali soggetti accedono nello Studio sarà indispensabile che operino sotto stretta sorveglianza e dovrà esser loro impedito di avere accesso agli archivi cartacei ed ai fascicoli non ancora riposti negli schedari; nell'ipotesi di tecnici software evitare che essi operino in modo da accedere alla visione degli archivi elettronici se non nelle misura strettamente necessaria per verificare l'integrità degli stessi o il funzionamento del programma.

SANZIONI

Un brevissimo cenno alle sanzioni irrogate nel caso di inosservanza in tema di informativa ed in tema di mancata adozione delle misure minime.
Nel primo caso si è in presenza di violazione amministrativa all'art. 161 del Codice; nel secondo caso si è in presenza di una fattispecie di reato colposo all'art. 169 del Codice.
L'**art. 161** del Codice della Privacy che così recita:
1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.
Le violazioni amministrative del Codice della Privacy trovano la loro disciplina generale nella materia degli illeciti amministrativi così come regolati dalla legge n. 689/81
Pertanto la violazione potrà ritenersi commessa allorquando l'omissione sia assistita dall'elemento psicologico quanto meno della colpa.
Quanto all'elemento oggettivo può essere riscontrato sia nella totale che parziale informativa.

Vi è chi ritiene che anche la tardiva informativa integri gli estremi della violazione; tuttavia poiché l'informativa potrà essere data anche oralmente sarà difficile provare che l'informativa sia stata data dopo l'inizio del trattamento.

L'art. 169 del Codice della Privacy così recita:

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili

Vertendosi in tema di reato punito a titolo di colpa, c'è chi ritiene che la disciplina dell'errore scusabile potrà trovare applicazione anche a tale ipotesi.

E' tuttavia possibile estinguere il reato nell'ipotesi di accertata commissione del reato attraverso il meccanismo disciplinato dal secondo comma della norma. Trattasi di una ipotesi di estinzione speciale rispetto all'oblazione disciplinata dall'art. 162 bis c.p.

Allegati:

Modello informativa
Modello informativa suggerito dal CNF
Modello autorizzazione del cliente
Modello documento programmatico della sicurezza
Modello documento programmatico della sicurezza suggerito dal CNF
Check list dei principali adempimenti
Tavola degli adempimenti e delle relative scadenze periodiche

Modello di informativa

Informativa ex art. 13 D.lgs. 196/2003
(Da inviare al cliente sotto forma di lettera)

Preg.mo sig./a,
Le comunico che il D.lgs. n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali") prevede la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

Ai sensi dell'articolo 13 del D.lgs. n.196/2003, pertanto, Le comunico quanto segue:

a) I dati personali – identificativi - sensibili e giudiziari, eventualmente acquisiti, anche, presso terzi, saranno utilizzati – nel rispetto della normativa vigente e fermi gli obblighi di riservatezza e di segreto professionale - esclusivamente per finalità di tipo legale / giudiziario in conformità allo scopo per cui è stato conferito mandato e, comunque, per finalità connesse e/o strumentali allo svolgimento degli incarichi professionali affidati allo studio legale *******, escluso – pertanto – ogni utilizzo diverso e/o confliggente con i Suoi ("*interessato*").

b) Il trattamento delle informazioni che La riguardano sarà improntato ai principi di correttezza, liceità, trasparenza e di tutela della riservatezza e saranno trattati e conservati con strumenti informatici (con modalità cartacee) .

c) Il conferimento dei dati personali – identificativi - sensibili e giudiziari deve intendersi quale mera facoltà e non obbligo.

d) Lo studio legale dell'avv. ******** ha redatto ed approntato un D.P.S. (Documento Programmatico della Sicurezza) nel quale sono descritte ed individuate le misure di sicurezza adottate per la sicurezza dei dati personali – identificativi – sensibili e giudiziari e gli eventuali aggiornamenti e/o modificazioni dei dati identificativi dei titolari, dei responsabili e/o degli incaricati

e) Gli estremi identificativi dei titolari del trattamento sono:

- Avv. _____, nato il _____a _____, cod.fisc. _____;
- Avv. _____, nato il _____a _____, cod.fisc. _____;
- Avv. _____, nato il _____a _____, cod.fisc. _____;

- ai sensi dell'articolo 4 lettera "g" quale "*responsabile del trattamento*" è nominato il Sig. _____ ; ogni modificazione del nominativo del responsabile verrà comunicata.

Infine, Le comunico che:

1. Il trattamento dei dati avverrà in modo idoneo a garantire la sicurezza e la riservatezza e potrà essere effettuato anche attraverso strumenti automatizzati che consentano la memorizzazione, la gestione e la trasmissione degli stessi.

2. I dati e la documentazione necessari e pertinenti agli incarichi in corso da instaurare o cessati verranno conservati, in archiviazione, oltre l'esecuzione degli incarichi affidati e precisamente per il periodo di 10 anni ed anche oltre tale periodo limitatamente ai dati personali per ragioni di carattere storico statistico e connesse al tipo di software utilizzato per la gestione dello Studio Legale e per la formazione dei testi.

3. I dati trattati attraverso strumenti automatizzati saranno invece cancellati all'esaurimento dell'incarico conferito, tranne quelli pertinenti e non eccedenti rispetto a successivi incarichi conferiti dal medesimo cliente ("*interessato*").

4. Si fa presente che è facoltà dell'interessato ex articolo 52 D.Lgs.n.196/2003 chiedere – secondo le modalità ed i termini in quella stessa norma indicati - che, per motivi legittimi, sia omessa l'indicazione delle generalità e di altri dati identificativi dello stesso nell'ipotesi di diffusione della eventuale sentenza o di altro provvedimento giurisdizionale.

Le comunico che il trattamento dei dati sensibili , identificativi e giudiziari richiede l'autorizzazione da parte Sua e la

mancata autorizzazione potrebbe rendere non espletabile il mandato conferito e conseguentemente il Suo rifiuto al trattamento e la conservazione dei dati, potrebbe comportare la rinuncia al mandato conferito per impossibilità alla prosecuzione dei giudizi in corso.

In ogni caso La informo che i dati non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione, fatta eccezione per i dati personali che per motivi fiscali si renderà necessari comunicare al commercialista dello Studio che ha dato assicurazione circa il rispetto del Codice della Privacy e della assoluta riservatezza oltre che dell'approntamento di un D.P.S. in conformità a quanto previsto dal citato Codice e dall'allegato B allo stesso Codice.

La informo che in ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'art.7 del D.lgs.196/2003, che per Sua comodità si riproduce in calce alla presente informativa

La informo che il conferimento dei suoi dati personali, sensibili, identificativi e giudiziari sono necessari per l'esercizio del mandato conferito onde consentire una adeguata difesa dei Suoi interessi e che, prescindendo dall'autorizzazione generale del Garante n. 04/2004, ritengo necessario che Lei conferisca espressa autorizzazione al trattamento dei dati personali, identificativi, sensibili e giudiziari.

Pertanto, La invito a prender contatti con il mio studio onde formalizzare l'autorizzazione ex d. l.vo 196/2003 preavvertendola che in difetto, potrei essere costretto a rimettere il mandato conferitomi se dovesse ravvisarsi la necessità, per una adeguata esecuzione dello stesso al trattamento e/o diffusione dei dati per i quali è necessaria la sua autorizzazione.

Di seguito si riportano le disposizioni del d. l.vo 196/03 che riguardano i Suoi diritti in materia di riservatezza dei dati personali, sensibili, identificativi e giudiziari.

1. ART.26 comma 4 lettera "c" – GARANZIE PER I DATI SENSIBILI: "[…] **4.** *I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:* ***c)*** *quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n.397, o – comunque - per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale il diritto deve essere di rango pari a quello dell'interessato ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile* […]".

2. ART.13 - INFORMATIVA: "***1.*** *L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente infirmati oralmente o per iscritto circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto; d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'articolo 7; f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art.7 è indicato tale responsabile.* ***2.*** *L'informativa di cui al comma 1 contiene ance gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento da parte di un soggetto pubblico di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.* ***3.*** *Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.* ***4.*** *Se i dati personali non sono raccolti presso l'interessato l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando,è prevista la loro comunicazione, non oltre la prima comunicazione.* ***5.*** *La disposizione di cui al comma 4 non si applica quando: a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla legge comunitaria; b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n.397 o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; c) l'informativa all'interessato comporta un impiego di mezzi che il Garante – prescrivendo eventuali misure appropriate – dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli – a giudizio del Garante – impossibile*".

3. ART.4 – DEFINIZIONI: "[…] ***b) <dato personale****>, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;* ***c)*** *<****dati identificativi****> i dati personali che permettono l'identificazione diretta dell'interessato;* ***d)*** *<****dati sensibili****>, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;* ***e)*** *<****dati giudiziari****>, i dati personali idonei a rivelare provvedimenti di cui all'art.3 comma 1, lettere da a) ad o) e da r) ad u) del D.P.R. 14.11.2002 n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61del codice di procedura penale*".

4. ART.4 – DEFINIZIONI: "[…] ***f)*** *<**titolare**>, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono – anche unitamente ad altro titolare . le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;* ***g)*** *<**responsabile**>, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;* ***h)*** *<**incaricati**>, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o responsabile*".

5. ART.7 – DIRITTO DI ACCESSO AI DATI PERSONALI ED ALTRI DIRITTI: "***1.*** *L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la loro comunicazione in forma intelligibile.* ***2.*** *L'interessato ha diritto di ottenere l'indicazione: a) dell''origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art.5 comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.* ***3.*** *L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero - quando via ha interesse – l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere da "a" a "b" sono state portate a conoscenza anche per quanto riguarda l loro contenuto di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.* ***4.*** *L'interessato ha diritto di opporsi in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento dei dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale*".

6. ART.25 – DIVIETI DI COMUNICAZIONE e DIFFUSIONE: "**1.** *La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'Autorità giudiziaria: a) in riferimento ai dati personali dei quali è stata ordinata la cancellazione, ovvero quanto è decorso il periodo di tempo indicato nell'art.11 comma 1, lettera "e"; b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.* ***2.*** *È fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza da altri soggetti pubblici ai sensi dell'art.58, comma 2, per finalità di difesa o sicurezza dello Stato o di prevenzione, accertamento o repressione di reati*".

7. ART.4 – DEFINIZIONI: "[…] ***a)*** *<**trattamento**> qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati anche se non registrati in una banca dati* […]; ***l)*** *<**comunicazione**> il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati in qualunque forma, anche mediante la loro messa a disposizione o consultazione;* ***m)*** *<**diffusione**> il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione*".

Luogo e data

(Firma)

Modello di informativa suggerito dal CNF

Informativa ai sensi dell'art. 13 d. lgs. 196/2003

Gentile Cliente, ai sensi dell'art. 13 d. lgs. 196/2003 (di seguito T.U.), ed in relazione ai dati personali di cui lo Studio _____ entrerà in possesso con l'affidamento della Sua pratica, La informiamo di quanto segue:

1. Finalità del trattamento dei dati.

Il trattamento è finalizzato unicamente alla corretta e completa esecuzione dell'incarico professionale ricevuto, sia in ambito giudiziale che in ambito stragiudiziale.

2. Modalità del trattamento dei dati.

a) Il trattamento è realizzato per mezzo delle operazioni o complesso di operazioni indicate all'art. 4 comma 1 lett. a) T.U.: raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco,comunicazione, cancellazione e distruzione dei dati.

b) Le operazioni possono essere svolte con o senza l'ausilio di strumenti elettronici o comunque automatizzati.

c) Il trattamento è svolto dal titolare e/o dagli incaricati del trattamento.

3. Conferimento dei dati.

Il conferimento di dati personali comuni, sensibili e giudiziari è strettamente necessario ai fini dello svolgimento delle attività di cui al punto 1.

4. Rifiuto di conferimento dei dati.

L’eventuale rifiuto da parte dell’interessato di conferire dati personali nel caso di cui al punto 3 comporta l’impossibilità di adempiere alle attività di cui al punto 1.

5. Comunicazione dei dati.

I dati personali possono venire a conoscenza degli incaricati del trattamento e possono essere comunicati per le finalità di cui al punto 1 a collaboratori esterni, soggetti operanti nel settore giudiziario, alle controparti e relativi difensori, a collegi di arbitri e, in genere, a tutti quei soggetti pubblici e privati cui la comunicazione sia necessaria per il corretto adempimento delle finalità indicate nel punto 1.

6. Diffusione dei dati.

I dati personali non sono soggetti a diffusione.

7. Trasferimento dei dati all’estero.

I dati personali possono essere trasferiti verso Paesi dell’Unione Europea e verso Paesi terzi rispetto all’Unione Europea nell’ambito delle finalità di cui al punto 1.

8. Diritti dell’interessato.

L’art. 7 T.U. conferisce all’interessato l’esercizio di specifici diritti, tra cui quello di ottenere dal titolare la conferma dell’esistenza o meno di propri dati personali e la loro messa a disposizione in forma intelligibile; l’interessato ha diritto di avere conoscenza dell’origine dei dati, della finalità e delle modalità del trattamento, della logica applicata al trattamento, degli estremi identificativi del titolare e dei soggetti cui i dati possono essere comunicati; l’interessato ha inoltre diritto di ottenere l’aggiornamento, la rettificazione e l’integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione della legge; il titolare ha il diritto di opporsi, per motivi legittimi, al trattamento dei dati.

9. Titolare del trattamento.

Titolare del trattamento è _____ con domicilio eletto in _____.

_____, lì _____

_____

Per ricevuta comunicazione

Io sottoscritto _____ autorizzo a norma degli art. 23 e 26 T.U. lo Studio _____ al trattamento dei miei dati personali comuni, sensibili e giudiziari.

_____, lì _____

_____

Per il rilasciato consenso

Modello Autorizzazione del cliente

DICHIARAZIONE DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI, IDENTIFICATIVI, SENSIBILI e GIUDIZIARI ex D.LGS. 30 giugno 2003 n.196

PERSONA FISICA

Io sottoscritto/a _____
nato/a il _____ a _____
residente a _____
in Via _____
cod.fisc. _____
qui di seguito identificato/a, anche, con il termine "*interessato/a*" nel significato di cui alla lettera "i" dell'art.4 D.Lgs.n.196/03 e cioè di: "*persona fisica, persona giuridica, ente o associazione cui si riferiscono i dati personali*".

PERSONA GIURIDICA

la Ditta / Società _____
con sede a _____
in Via _____
cod.fisc. / partita I.V.A. _____
in persona di _____
nella sua qualità di _____
nato/a il _____ a _____
residente a _____
in Via _____
cod.fisc. _____
qui di seguito identificata, anche, con il termine "*interessato*" nel significato di cui alla lettera "i" dell'art.4 D.Lgs.n.196/03 e cioè di: "*persona fisica, persona giuridica, ente o associazione cui si riferiscono i dati personali*".

DICHIARA

di avere conferito incarico allo studio legale dell'avv. **** per la tutela dei suoi interessi ed affari economico-giuridici, riservando per l'espletamento di attività giurisdizionali il rilascio di apposito mandato ed esplicitando che la presente non costituisce mandato generale alle liti

Ai sensi e per gli effetti di quanto previsto dal d. l.vo n. 196 del 30/06/2003, il sottoscritto (nella sua qualità) dichiara di essere stato edotto dall'avv. ***** circa il contenuto dell'art. 23 d. l.vo n. 196 del 30/06/2003 ed in particolare, circa il consenso espresso che deve essere manifestato dall'interessato per il trattamento dei dati personali preceduto dall'informativa di cui all'articolo 13 D.Lgs.n.196/03, e circa il consenso espresso e per iscritto dei dati c.d. "sensibili" tranne nelle ipotesi di cui all'art.26 comma 4 lettera "c" il cui contenuto dichiara di conoscere ed il cui testo riconosce essere quello riportato alla **nota 1** posta in calce alla presente autorizzazione.

Conseguentemente il sottoscritto, in ottemperanza al disposto normativo di cui all'articolo 13 ("*Informativa*") del D.Lgs.n.196/03, il cui contenuto dichiara di conoscere ed il cui testo integrale riconosce essere quello riportato alla **nota 2** posta in calce alla presente autorizzazione, dichiara di essere stato previamente informato di quanto segue:

1. I dati personali – identificativi - sensibili e giudiziari (il cui rispettivo significato è stato illustrato al sottoscritto che riconosce essere quello riportato alla **nota 3** posta in calce alla presente autorizzazione), eventualmente acquisiti, anche, presso terzi, saranno utilizzati – nel rispetto della normativa vigente e fermi gli obblighi di riservatezza e di segreto professionale - esclusivamente per finalità di tipo legale / giudiziario in conformità allo scopo per cui verrà conferito mandato e, comunque, per finalità connesse e/o strumentali allo svolgimento degli incarichi professionali affidati allo studio legale *******, escluso – pertanto – ogni utilizzo diverso e/o confliggente con gli interessi del Cliente ("*interessato*").

2. Il trattamento delle informazioni che riguardano il sottoscritto sarà improntato ai principi di correttezza, liceità, trasparenza e di tutela della riservatezza e saranno trattati e conservati con strumenti informatici (con modalità cartacee) .

3. Il conferimento dei dati personali – identificativi - sensibili e giudiziari deve intendersi quale mera facoltà e non obbligo.

4. In mancanza di conferimento dei dati succitati il mandato ed in generale gli incarichi e/o prestazioni professionali richieste – oltre che la prosecuzione di quelli/e in corso - potranno non essere accettati e/o continuati e, dunque, espletati.

5. Qualora venga autorizzato il trattamento dei dati personali – identificativi - sensibili e giudiziari, questi, nell'espletamento del mandato e/o dell'incarico professionale conferito e, comunque, nei limiti e per le finalità del

punto “a” che precede, potranno venire a conoscenza di soggetti Pubblici e/o Privati, delle competenti Autorità Giudiziarie e, quindi, dei soggetti in quelle stesse sedi preposti al loro recepimento e/o trattamento, oltre che, per quanto riguarda lo studio legale ***** , dagli avvocati titolari, dagli eventuali responsabili e/o incaricati designati (le cui funzioni mi sono state specificate e riconosco essere quelle riportate alla **nota 4** posta in calce alla presente autorizzazione), oltre che dai collaboratori di studio, dai praticanti e dalle segretarie che potranno trattare i dati personali dei Clienti (“*interessati*”) anche ai fini della redazione delle note spese.

6. Lo studio legale dell’avv. ******** ha redatto ed approntato un D.P.S. (Documento Programmatico della Sicurezza) nel quale sono descritte ed individuate le misure di sicurezza adottate per la sicurezza dei dati personali – identificativi – sensibili e giudiziari e gli eventuali aggiornamenti e/o modificazioni dei dati identificativi dei titolari, dei responsabili e/o degli incaricati.

7. In caso di sottoscrizione dell'autorizzazione al trattamento dei dati, all’interessato saranno garantiti tutti i diritti così come meglio specificati all’art.7 (“*Diritto di accesso ai dati personali ed altri diritti* ”) D.Lgs.n.196/03 il cui contenuto dichiaro di conoscere ed il cui testo integrale riconosco essere quello riportato alla **nota 5** in calce alla presente autorizzazione.

8. Gli estremi identificativi dei titolari del trattamento sono:

   - Avv. _____, nato il _____a _____, cod.fisc. _____;
   - Avv. _____, nato il _____a _____, cod.fisc. _____;
   - Avv. _____, nato il _____a _____, cod.fisc. _____;

   - ai sensi dell’articolo 4 lettera “g” quale “*responsabile del trattamento*” è nominato il Sig. _____ ; ogni modificazione del nominativo del responsabile verrà comunicata.

Il sottoscritto dichiara, altresì, di essere stato edotto che, qualora venisse autorizzato il trattamento dei dati personali – identificativi - sensibili e giudiziari, questi, nell’espletamento del mandato conferito e salvo quanto previsto nei punti che seguono, nei limiti di legge così come stabiliti ex art.25 D.Lgs.n.196/03 il cui contenuto dichiaro di conoscere ed il cui testo riconosco essere quello riportato alla **nota 6** posta in calce alla presente autorizzazione, nonché per le finalità di cui al punto “a”, potranno essere soggetti, oltre che a trattamento, anche a comunicazione e/o diffusione nel significato tecnico così come meglio illustrato alle lettere “a”, “l” ed “m” del comma 1 dell’art.4 D.Lgs.n.196/03 e che riconosco essere quello di cui alla **nota 7** posta in calce alla presente autorizzazione.

Infine, al sottoscritto è stata data comunicazione che:

1. Il trattamento dei dati avverrà in modo idoneo a garantire la sicurezza e la riservatezza e potrà essere effettuato anche attraverso strumenti automatizzati che consentano la memorizzazione, la gestione e la trasmissione degli stessi.

2. I dati e la documentazione necessari e pertinenti agli incarichi in corso da instaurare o cessati verranno conservati, in archiviazione, oltre l’esecuzione degli incarichi affidati e precisamente per il periodo di 10 anni ed anche oltre tale periodo limitatamente ai dati personali per ragioni di carattere storico statistico e connesse al tipo di sofware utilizzato per la gestione dello Studio Legale e per la formazione dei testi.

3. I dati trattati attraverso strumenti automatizzati saranno invece cancellati all’esaurimento dell’incarico conferito, tranne quelli pertinenti e non eccedenti rispetto a successivi incarichi conferiti dal medesimo cliente (“*interessato*”).

4. E’ facoltà dell’interessato ex articolo 52 D.Lgs.n.196/2003 chiedere – secondo le modalità ed i termini in quella stessa norma indicati - che, per motivi legittimi, sia omessa l’indicazione delle generalità e di altri dati identificativi dello stesso nell’ipotesi di diffusione della eventuale sentenza o di altro provvedimento giurisdizionale.

5. La sottoscrizione della presente autorizzazione al trattamento dei dati personali – identificativi - sensibili e giudiziari, dovrà ritenersi valida anche per le posizioni aperte prima del 01.01.2004.

Pertanto il sottoscritto preso atto di quanto sopra dichiarato e confermandolo espressamente

AUTORIZZA

lo Studio Legale dell’avv. **** e per esso il titolare del trattamento dei dati, il responsabile del trattamento e gli incaricati in conformità a quanto sopra indicato e più in generale secondo quanto previsto ex D.Lgs.n.169/03, al

trattamento dei propri dati personali di qualsiasi natura ivi compresi quelli c.d. sensibili, identificativi e giudiziari, ivi comprese le modalità descritte in tutta la parte che precede, confermando – altresì – che per l'eventuale fase giudiziale verrà rilasciato apposito mandato nelle forme di legge. Altresì il sottoscritto **conferma espressamente di autorizzare** lo Studio Legale dell'avv. *** e per esso il titolare del trattamento dei dati, il responsabile del trattamento e gli incaricati, alla conservazione dei propri dati personali anche successivamente l'esecuzione e l'esaurimento degli incarichi affidati con divieto di comunicazione e diffusione purchè per ragioni di carattere statistico e storico con eccezione di ragioni di carattere fiscale.
Infine, il sottoscritto **autorizza** lo Studio Legale dell'avv. **** e per esso il titolare del trattamento dei dati, il responsabile del trattamento e gli incaricati a comunicare i propri dati personali al commercialista e/o al soggetto persona fisica o giuridica che gestisce la contabilità dello Studio Legale e redige le dichiarazioni fiscali al solo fine di far fronte ai necessari adempimenti fiscali

Andria lì _____

F.to L'INTERESSATO

Note richiamate nell'Autorizzazione che precede,
lette ed esplicitate mediante precisa spiegazione al sottoscritto

1. ART.26 comma 4 lettera "c" – GARANZIE PER I DATI SENSIBILI: "[…] **4.** *I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:* ***c)*** *quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n.397, o – comunque - per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale il diritto deve essere di rango pari a quello dell'interessato ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile* […]".
2. ART.13 - INFORMATIVA: "***1.*** *L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente infirmati oralmente o per iscritto circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto; d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'articolo 7; f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art.7 è indicato tale responsabile.* ***2.*** *L'informativa di cui al comma 1 contiene ance gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento da parte di un soggetto pubblico di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.* ***3.*** *Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.* ***4.*** *Se i dati personali non sono raccolti presso l'interessato l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando,è prevista la loro comunicazione, non oltre la prima comunicazione.* ***5.*** *La disposizione di cui al comma 4 non si applica quando: a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla legge comunitaria; b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n.397 o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; c) l'informativa all'interessato comporta un impiego di mezzi che il Garante – prescrivendo eventuali misure appropriate – dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli – a giudizio del Garante – impossibile*".
3. ART.4 – DEFINIZIONI: "[…] ***b) <dato personale>****, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;* ***c)*** *<**dati identificativi**> i dati personali che permettono l'identificazione diretta dell'interessato;* ***d)*** *<**dati sensibili**>, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;* ***e)*** *<**dati giudiziari**>, i dati personali idonei a rivelare provvedimenti di cui all'art.3 comma 1, lettere da a) ad o) e da r) ad u) del D.P.R. 14.11.2002 n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61del codice di procedura penale*".

4. ART.4 – DEFINIZIONI: "[…] ***f)*** *<**titolare**>, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono – anche unitamente ad altro titolare . le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;* ***g)*** *<**responsabile**>, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;* ***h)*** *<**incaricati**>, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o responsabile*".

5. ART.7 – DIRITTO DI ACCESSO AI DATI PERSONALI ED ALTRI DIRITTI: "***1.*** *L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la loro comunicazione in forma intelligibile.* ***2.*** *L'interessato ha diritto di ottenere l'indicazione: a) dell''origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art.5 comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.* ***3.*** *L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero - quando via ha interesse – l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere da "a" a "b" sono state portate a conoscenza anche per quanto riguarda l loro contenuto di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.* ***4.*** *L'interessato ha diritto di opporsi in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento dei dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale*".

6. ART.25 – DIVIETI DI COMUNICAZIONE e DIFFUSIONE: "**1.** *La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'Autorità giudiziaria: a) in riferimento ai dati personali dei quali è stata ordinata la cancellazione, ovvero quanto è decorso il periodo di tempo indicato nell'art.11 comma 1, lettera "e"; b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.* ***2.*** *È fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza da altri soggetti pubblici ai sensi dell'art.58, comma 2, per finalità di difesa o sicurezza dello Stato o di prevenzione, accertamento o repressione di reati*".

7. ART.4 – DEFINIZIONI: "[…] ***a)*** *<**trattamento**> qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati anche se non registrati in una banca dati* […]; ***l)*** *<**comunicazione**> il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati in qualunque forma, anche mediante la loro messa a disposizione o consultazione;* ***m)*** *<**diffusione**> il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione*".

F.to L'INTERESSATO

Modello di Documento Programmatico della Sicurezza

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA PER L'ANNO _____

Il presente documento delinea il quadro delle misure di sicurezza, organizzative, fisiche e logiche, che lo Studio Legale dell'avv. ***** adotta per il trattamento dei dati personali effettuato, in conformità ed Ai sensi e per gli effetti dell'art. 34, comma 1, lettera g) del decreto legislativo n.196 del 20 giugno 2003, e del disciplinare tecnico allegato al medesimo decreto

Indice

ORGANIGRAMMA

TITOLARE DEL TRATTAMENTO (Art. 28 d. l.vo 196/03)

Titolare del trattamento dei dati personali, sensibili, identificativi e giudiziari è l'avv. ******

RESPONSABILE DEL TRATTAMENTO (Art. 29 d. l.vo 196/03)

Responsabile del trattamento dei dati personali, sensibili, identificativi e giudiziari è l'avv. ******

INCARICATI DEL TRATTAMENTO (Art. 30 d. l.vo 196/03)

Incaricati del trattamento sono:

Avv……..(collaboratore o socio dello studio)

Dr. …… (collaboratore o praticante di studio)

Dr. …… (collaboratore o praticante di studio)

……. (dipendente)

…….. (dipendente)

Amministratore del Sistema è……..

Custode delle Password è …….

Tecnico incaricato dell'assistenza e manutenzione degli strumenti elettronici è …….

ELENCO DATI TRATTATI (punto 19.1 Allegato B al d. l.vo 196/03)

Lo Studio Legale tratta i seguenti dati personali anche attraverso soggetti terzi appositamente incaricati per specifiche attività quali investigatori privati; avvocati, operanti in altri sedi, associati alla difesa del cliente; soggetti esercenti attività di gestione di pratiche immobiliari o auto ecc. divisi per tipologia di interessato:

Cliente	dati identificativi, comuni, sensibili e giudiziari ivi compresi quelli ricavati da albi, elenchi e registri pubblici, visure camerali; visure e certificazioni ipo-catastali, nonché i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi; quelli forniti dagli stessi per lo svolgimento dell'attività di difesa; quelli sensibili idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico; quelli sensibili idonei a rivelare lo stato di salute e la vita sessuale; quelli giudiziari e quelli idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, ovvero idonei a rivelare al qualità di imputato o indagato
Terzi	dati identificativi comuni, sensibili e giudiziari di terzi intendendosi per tali le controparti, i fornitori, i corrispondenti forniti dai clienti o reperiti attraverso indagini difensive o pubblici uffici; ivi compresi quelli necessari per l'esercizio dell'attività di difesa ed in ossequio al mandato ricevuto, compresi i dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari; quelli idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, ovvero idonei a rivelare al qualità di imputato o indagato; quelli sensibili idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico; quelli sensibili idonei a rivelare lo stato di salute e la vita sessuale; quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria
Personale dipendente, collaboratori, praticanti,professionisti associati.	dati identificativi, personali e sensibili necessari per lo svolgimento del rapporto di lavoro, reperibilità e necessità di corrispondenza a fini fiscali e previdenziali ovvero di natura bancaria e quelli sensibili idonei a rivelare lo stato di salute e quelli idonei a rivelare l'appartenenza ad organizzazioni sindacali, ove necessario

Modalità in cui avviene il trattamento.

Il trattamento dei dati effettuato dallo studio che, per quelli non pubblici vengono acquisiti previa l'informativa che si allega al presente D.P.S., avverrà per il tempo necessario all'espletamento dell'incarico ricevuto ovvero per il tempo necessario per l'assolvimento di obblighi di legge ed in funzione degli scopi di raccolta ovvero per ragioni di natura statistica e/o storico.

Il trattamento si sostanzia nelle seguenti operazioni:

- Raccolta consistente nell'acquisizione e reperimento dei dati direttamente dall'interessato ovvero su sua indicazione ovvero attraverso indagini presso terzi ovvero indirettamente;

- registrazione, organizzazione ed elaborazione dei dati attraverso il loro inserimento in supporti informatici o cartacei;
- consultazione, selezione, estrazione ed utilizzo dei dati a seconda dell'uso necessario per lo svolgimento del mandato e per le esigenze difensive;
- raffronto e modificazione dei dati attraverso il loro aggiornamento;
- interconnessione, comunicazione e diffusione dei dati a seconda dell'uso necessario per lo svolgimento del mandato e per le esigenze difensive
- conservazione ed archiviazione dei dati nei supporti informatici posizionati in modo da garantire la riservatezza e la sicurezza dei dati, collegati tra loro in rete locale e con accesso ad internet ovvero in supporti cartacei consistenti fascicoli riposti in schedari dotati di chiusura;
- blocco dei dati nell'ipotesi in cui possa pregiudicarsi il diritto dell'interessato;
- cancellazione dei dati dai supporti informatici ovvero la loro distruzione dai supporti cartacei una volta terminato il loro trattamento.

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' TRA I SOGGETTI CHE HANNO ACCESSO AI DATI (punto 19.2 Allegato B al d. l.vo 196/03).

Premesso che tutti i dati trattati in modo cartaceo dallo Studio sono conservati in apposite cartelle, in archivi ubicati in ambienti rigorosamente separati dal luogo di ricevimento della clientela e che i dati trattati con strumenti informatici sono conservati in supporti accedibili con appositi profili di autorizzazione specificatamente ed individualmente determinati, la distribuzione dei compiti e delle responsabilità avviene nel modo che segue.

		Titolare	Respon-sabile	Ammini-stratore di sistema	Incaricato addetto alla Segreteria	Incaricato addetto alla contabilità	Praticanti	Terzi (commer-cialista; corrispon-denti; collabora-tori ecc.)
CLIENTE	Dati comuni							
	Dati sensibili							
	Dati giudiziari							
	Dati idonei a rivelare stato di salute e vita sessuale							

TERZO	Dati comuni							
	Dati sensibili							
	Dati giudiziari							
	Dati idonei a rivelare stato di salute e vita sessuale							
COLLABORATORICORRISPONDENTI,DIPENDENTI,PRATICANTI,	Dati comuni							
	Dati sensibili							
	Dati giudiziari							
	Dati idonei a rivelare stato di salute o appartenenza a organismi sindacali							

Il **custode delle password** non ha un autonomo accesso e diritto al trattamento dei dati salvo le diverse mansioni cui è designato.
Il **tecnico incaricato dell'assistenza e manutenzione degli strumenti elettronici** accede e tratta i dati solo stretta sorveglianza del Titolare o del Responsabile e limitatamente per la verifica della integrità degli stessi e per la piena funzionalità dei programmi (software) di trattamento.
Il trattamento dei dati giudiziari comprende anche quelli idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, ovvero idonei a rivelare al qualità di imputato o indagato.
Il trattamento dei dati effettuato dagli incaricati (addetti alla Segreteria, corrispondenti, commercialista esterno) anche allorquando relativo a quelli sensibili o giudiziari, ovvero quelli afferenti i pagamenti a favore di terzi fornitori e conseguenti rapporti bancari, avviene su disposizione del titolare in via generale ovvero su espressa autorizzazione del titolare di volta in volta in funzione delle mansioni all'uopo assegnategli e per il tempo strettamente necessario all'incarico affidato.
Tutti coloro che sono autorizzati al trattamento dei dati sono stati resi edotti circa le responsabilità di natura patrimoniale, sanzionatoria amministrativa e penale circa il trattamento effettuato in disprezzo delle istruzioni ricevute, circa la divulgazione non autorizzata dei dati e circa il

trattamento illecito degli stessi. All'uopo a tutti gli incaricati si è rilasciato apposita comunicazione allegata al presente D.P.S. sotto la lettera ******

ANALISI DEI RISCHI (punto 19.3 Allegato B al d. l.vo 196/03).

Prima di procedere all'analisi dei rischi, si è proceduto ad una ricognizione della struttura, delle attrezzature e degli strumenti informatici

Descrizione della struttura

L'immobile ove è ubicato lo Studio Legale (per comodità denominato studio), è al primo piano di un condominio in zona centrale, dotato di portone di ingresso a chiusura automatica e con videocitofono, con sorveglianza notturna, e porte blindate.
La segreteria è ubicata in un locale più ampio, dove in una zona separata e ben distanziata dalle postazioni di lavoro delle segretarie, è ricavata una sala di attesa per i clienti.
All'interno dell'immobile vi sono stanze costituenti singoli studi, ove operano i singoli componenti dello Studio siano essi avvocati, praticanti e/o collaboratori fissi; ognuna di queste stanze è dotata di porta con chiusura a chiave.

Descrizione degli archivi cartacei
Le singole pratiche sono racchiuse in cartelle contenenti tutti i dati e i documenti relativi all'incarico ricevuto e conservati in schedari dotati di chiusura a chiave posti nell'archivio ubicato in stanza separata dotata di porta con chiusura a chiave
Lo studio è munito di cassaforte con chiusura a chiave in zona riservata.

Descrizione degli strumenti elettronici
Lo Studio è dotato di un computer marca …….. modello …… che funge da server ubicato nella stanza ove sono ubicati gli archivi cartacei.
Ogni stanza dello Studio è attrezzata di computer terminali di tipo intelligente collegati al server ed agli altri computer terminali di tipo intelligente in rete locale, connessi ad internet con ADSL, eccezione fatta per la sala biblioteca dove sono ubicati due computer terminali di tipo intelligente in rete locale e con connessione ADSL ad internet; nel più ampio locale, destinata a segreteria si trovano due postazioni di lavoro con computer terminali di tipo intelligente in rete locale e con connessione ADSL ad internet.
Le linee telefoniche sono due ISDN, oltre la linea ADSL, per la connessione ad internet gestita da un router marca ……...
Inoltre in questo locale si trovano le seguenti stampanti marca…….;
il fax marca……;
la fotocopiatrice marca…….
lo scanner marca ……...;
Il computer della segreteria utlizzato da……. è dotato di separato modem marca ……. per l'utilizzo di Winfax.
In particolare:
nr. 1 computer connesso in rete ed a internet nella segreteria marca …….. modello …… è utilizzato da …….
nr. 1 computer connesso in rete ed a internet nella segreteria marca …….. modello …… è utilizzato da …….
nr. 1 computer connesso in rete ed a internet nella segreteria marca …….. modello …… è utilizzato da …….

nr. 1 computer connesso in rete ed a internet marca …….. modello ……nello studio dell'avv. …… è utilizzato da …….
nr. 1 computer connesso in rete ed a internet marca …….. modello ……nello studio dell'avv. …… è utilizzato da …….
nr. 1 computer connesso in rete ed a internet nella biblioteca marca ……. modello ……..
nr. 1 computer connesso in rete ed a internet nella biblioteca utilizzato da …….. marca …. modello ……..
Il sistema operativo del server è ……..
Il sistema operativo dei computer è……
Lo studio adopera Internet Explorer versione …..
Lo studio adopera per la messaggistica di posta elettronica Outlook Express versione ……..
Lo studio per la gestione informatica delle pratiche e delle incombenze connesse con l'esercizio della professione utilizza il seguente programma ……..
Antivirus adoperato ……..
Firewall adoperato …….
Infine lo Studio è dotato di un impianto di videosorveglianza marca……. modello ……. Le immagini sono /non sono registrate e salvate in videocassette / supporti magnetici e conservati per giorni …… decorsi i quali vengono cancellate.
Dopo avere effettuato la ricognizione della struttura e delle apparecchiature in possesso dello studio, si è proceduto alla concreta analisi dei rischi ed alla loro quantizzazione.
Nell'analisi si attribuita uguale importanza ai dati senza operare distinzione tra i dati comuni ed i dati sensibili. Tale scelta è stata giustificata dalla volontà di attribuire un eguale grado di sicurezza a tutti i dati trattati dallo Studio e per evitare distingui, forieri di errori.
Si è così pervenuti alla seguente stima del grado di rischio senza distinzione tra trattamento dei dati con l'ausilio o senza l'ausilio di strumenti informatici, essendo gli stessi tra loro assimilabili.

Tipo di rischio	**Grado di rischio**			
	Molto alto	Alto	Medio	Basso
Rischi di distruzione o perdita, anche accidentale dei dati;				
Rischi furto e/o accesso non autorizzato ai dati;				
Rischi di trattamento non consentito o non conforme alla finalità della raccolta, ivi compresi i comportamenti fraudolenti diretti alla diffusione, trasmissione, asporto e sabotaggio dei dati				
Rischi connessi alla violazione e manipolazione dei dati, ivi comprese le violazioni, il furto e le intercettazioni delle credenziali di autenticazione				
Rischi connessi alla connessione in rete degli strumenti elettronici intesi sia quelli di connessione alla rete locale che ad internet ivi compresi i rischi derivanti dalla violazione del sistema informatico da malware e spamming e l'intercettazione dei dati contenuti nei supporti informatici				
Rischi connessi all'uso improprio degli strumenti informatici.				
Rischi connessi da disattenzioni, incuria ed errori nel trattamento dei dati				
Rischi connessi all'integrità dei supporti di archiviazione e di registrazione dei dati sull'hard disk				
Rischi connessi alla violazione dei fascicoli di studio e dei documenti ivi contenuti				
Rischi connessi all'accesso non autorizzato ed all'utilizzo improprio delle cartelle contenute nell'archivio				
Rischi connessi da errori umani nella gestione della sicurezza				

Rischi di accesso non autorizzato nella struttura				
Rischi connessi con incendi, furti ed eventi accidentali che possano danneggiare la struttura, gli impianti tecnologici (impianto elettrico, condutture del gas, climatizzatore, ecc.), gli strumenti informatici e gli archivi cartacei				

MISURE ADOTTATE PER PREVENIRE I RISCHI ANALIZZATI (art. 19.4 Allegato B al d. l.vo 196/03)

Per ridurre i rischi sono state adottate le seguenti misure:

Protezione dello Studio e della struttura
L'accesso allo studio è controllato; lo studio è dotato di videocitofono e chiusura con porta blindata.
Lo studio ha un contratto di assistenza e telesorveglianza con la ditta …….
L'accesso alle singole stanze è garantito da porte con chiusura e l'eventuale ingresso di terzi estranei avviene solo previa accettazione e controllo.
L'accesso ai singoli strumenti da parte di persone non autorizzate è impedito poiché gli stessi sono controllati dagli utenti autorizzati; la zona di attesa dei clienti è distanziata dagli strumenti essendo gli stessi clienti controllati dagli addetti alla Segreteria.
Il locale destinato all'archivio cartaceo è chiuso a chiave.
L'accesso all'archivi cartaceo è controllato dal Titolare ed in sua assenza dall'incaricato all'uopo nominato.
Fuori dall'orario di lavoro l'accesso all'archivio è consentito previa registrazione.
Per prevenire eventi naturali accidentali quali incendi, allagamenti e corto circuiti si è proceduto ad adottare tutte le cautele previste dalla normativa in tema di sicurezza degli impianti tecnologici e l'impianto elettrico è dotato di dispositivi salvavita.
Si è provveduto a dotare lo Studio di un dispositivo tritadocumenti nel quale vengono trinciati i documenti; tutti gli appunti e le fotocopie mal riuscite vengono distrutte con l'apposito dispositivo tritadocumenti.
I fascicoli d'ufficio vengono utilizzati per il tempo strettamente necessario allo svolgimento dell'incarico affidato e nell'ipotesi di ricevimento della clientela, gli stessi vengono chiusi per evitare letture indesiderate dei dati contenuti ovvero la lettura a contrario dei documenti.

Protezione degli strumenti informatici.
Autenticazione informatica. Tale misura è stata adottata dotando ciascun incaricato di una password di almeno 8 caratteri (o minore per le caratteristiche del sistema). Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né allo studio legale. La password viene autonomamente scelta dall'incaricato e dallo stesso custodita in una busta chiusa che viene consegnata al custode delle password ovvero al titolare del trattamento, il quale provvede a metterla nella cassaforte dello studio in un plico sigillato. Ogni tre mesi ciascun incaricato provvede a sostituire la propria password. Si è altresì disposto che le password vengano automaticamente disattivate dopo tre mesi di non utilizzo.
Si è prevista la immediata disattivazione delle credenziali di autenticazione nell'ipotesi di l'incaricato perda la sua qualità
Inoltre si è disposto che a tutti gli incaricati utilizzatori di strumenti elettronici non lascino incustodito, o accessibile, lo strumento elettronico stesso.
A tale riguardo, per evitare errori e dimenticanze, è stato disposto l'inserimento di uno screensaver automatico dopo 1 minuto di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
Si è inoltre disposto che gli incaricati verifichino la provenienza delle e-mail e non effettuino operazioni di file sharing.

Si è vietata la navigazione in internet se non in siti istituzionali e specifici di oggetto giuridico; si è vietata l'apertura di e-mail sospette e si è data istruzione per la verifica della provenienza della posta elettronica.
Si è data istruzione di non fornire alcun dato a chiunque telefoni quandanche si qualificasse come soggetto agente per ordine del giudice ovvero come incaricato del gestore telefonico per prevenire attacchi di social engineering.
Non si è provveduto alla creazione di credenziali di autenticazione separate per ogni incaricato, preferendo creare separate credenziali di autorizzazione separate per computer. La ragione di questa scelta è stata determinata dalla limitata dimensione dello Studio nel quale tutti gli incaricati, nella generalità hanno accesso e trattano tutti i dati in funzione delle funzioni e mansioni assegnate e per la stabilità dell'apparecchiatura concessa in uso ad ogni singolo operatore.
Per evitare i rischi derivanti da attacchi informatici ogni singolo computer è dotato di dispositivo antivirus di marca ……., che viene aggiornato con funzione automatica e con scansione di aggiornamento settimanale; inoltre sul server e sui computer terminali intelligenti è stato installato firewall di marca …….
Per ogni singolo computer è prevista la funzione di aggiornamento automatico del sistema fornito dalla Microsoft mediante lo strumento windows – update.
Analogo sistema di aggiornamento automatico è previsto per l'antivirus. E' stata data istruzione che, qualora nessun aggiornamento del sistema fosse segnalato automaticamente per un periodo di mesi 6, si provveda comunque ad attivare la funzione di controllo per verificare l'esistenza o meno di detti aggiornamenti automatici.
Si è data istruzione di non consentire la visione del video a terzi estranei allo staff dello Studio e nell'ipotesi in cui vengano effettuate le pulizie dello Studio i computer siano spenti.
Per evitare i rischi connessi con la perdita di dati contenuti negli strumenti informatici durante la registrazione o il trattamento, per interruzione dell'energia elettrica, lo Studio è stato dotato di un gruppo di continuità del tipo 0 waite state marca ……
Per prevenire i rischi da errori umani, si è provveduto ad istruire tutti gli incaricati circa il comportamento da tenere per prevenire pericoli ed errori; quanto ai pericoli per uso infedele delle apparecchiature e comportamento doloso si è provveduto alla scelta di incaricati scrupolosi, fedeli e professionalmente preparati.

Protezione dei dati cartacei
Si è disposto che qualsiasi documento che i Sig.ri Clienti consegnino allo Studio vada inserito in apposite cartelline non trasparenti; che qualsiasi documento che lo Studio consegni ai Sig.ri Clienti vada inserito in apposite buste o cartelline non trasparenti.
Si è disposto che le rubriche telefoniche in utilizzo su supporto cartaceo siano richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non contenga alcun dato (praticamente il primo foglio funge da copertina).
Si è disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche.
Si è disposto che i fascicoli vadano conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti.
Si è data istruzione di interrompere la sessione di lavoro e di chiudere i fascicoli quando vengano ricevuti i clienti durante una sessione di lavoro, questo sia interrotto ed il fascicolo sia chiuso per evitare la lettura di dati e documenti dello stesso anche attraverso una lettura a rovescio da parte del terzo o altro cliente.
Si è disposto che i telefax inviati su carta chimica siano riprodotti su carta normale per evitarne il deterioramento.
Si è disposto che le comunicazioni a mezzo posta, o a mezzo telefax, siano tempestivamente smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato e consegnato all'interessato.

Si è data istruzione che il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia distrutto con l'apposito tritadocumenti e riposto in appositi sacchi di plastica e che detti sacchi siano chiusi in modo che comunque atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detto materiale sia giornalmente asportato ovvero asportato secondo la normativa locale per la raccolta di rifiuti.
Per quanto riguarda la documentazione cartacea, si è disposto che l'archivio sia chiuso a chiave, gli schedari chiusi, e siano adottate le altre misure indicate.
Si è data istruzione di procedere alla restituzione dei documenti originali al cliente e di eliminare fisicamente il fascicolo cartaceo salva la conservazione di quanto ivi ancora contenuto per motivi storici, statistici e purchè segretamente conservato ed i dati non siano oggetto di trattamento ad eccezion fatta per ragioni di carattere fiscale ovvero per altri adempimenti di legge.
Si è data istruzione di non portare fuori dallo Studio i documenti cartacei e nell'ipotesi in cui fosse strettamente necessario che i fascicoli siano tenuti sotto controllo per evitare smarrimenti.
Si è disposto di non utilizzare le fotocopie dei documenti ivi comprese quelle mal riuscite contenente qualsiasi dato di clienti o terzi quale carta per appunti e che dopo l'utilizzo delle stesse vengano distrutte nel tritadocumenti.
Si è data istruzione di non dare divulgazione nemmeno a titolo di esempio delle pratiche trattate nello Studio

Personale addetto all'uso degli strumenti informatici ed all'uso dei documenti cartacei
Si attesta che gli incaricati al trattamento dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi,
Inoltre i dati, quanto comuni che sensibili, per gli affari trattati dallo Studio ed il tipo di clientela dello Studio non paiono essere di particolare interesse per terzi.

CONTINGENCY PLANNING E DISASTER RECOVERY
(punto 19.5 Allegato B al d. l.vo 196/03)

Si sono impartite le seguenti istruzioni:
- avvertire il titolare del trattamento dei dati e l'incaricato che ha in custodia il c.d. di back up, nonché i c.d. contenenti i vari software dello studio installati sugli strumenti elettronici;
- rivolgersi immediatamente e chiedere l'intervento del tecnico manutentore della ditta ……. ……. sollecitandone al più presto l'assistenza;
- provvedere a ripristinare tutti i dati contenuti nei supporti di back up una volta che si sono reinstallati i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware,;
- provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
- eseguire tutti le misure ed i suggerimenti ricevuti dal tecnico manutentore;
- effettuare il ripristino dei dati e dei sistemi entro e non oltre 7 giorni;
- predisporre almeno due volte l'anno un intervento di manutenzione de tecnico incaricato per verificare l'integrità degli strumenti informatici usati e l'integrità del software.

FORMAZIONE DEGLI INCARICATI
(punto 19.6 Allegato B al d. l.vo 196/03)

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali.

Inoltre, essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile o giudiziaria.
La formazione comprende la spiegazione di tutte le istruzioni dirette alla tutela della riservatezza ed alla tutela dei dati per evitare che gli stessi possano essere involontariamente resi disponibili a terzi.
La formazione è fatta dal titolare dello studio.

DATI PERSONALI E SENSIBILI AFFIDATI A TERZI
(art. 19.7 Allegato B al d. l.vo 196/03)

Si è data istruzione e ci si è accertati che i terzi, cui sono affidati i dati dei clienti dello Studio, ivi compreso il commercialista ovvero lo Studio commerciale che gestisce la contabilità dello Studio e gli avvocati corrispondenti associati alla difesa, nel caso in cui il trattamento dei dati sensibili e/o giudiziari siano trattati con strumenti elettronici, abbiano garantito di avere adottato le misure minime di sicurezza, attraverso il rilascio di apposita dichiarazione attestante l'adozione delle predette misure minime di sicurezza previste dal disciplinare.
Alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei allo studio, viene dato incarico scritto con richiesta di specificazione dei nominativi delle persone che accedono ed espresso invito a limitarsi alle sole attività pertinenti alla prestazione per cui accedono.
In ogni caso si è data istruzione agli incaricati di vigilare sulla presenza di terzi nello Studio.
Nell'ipotesi di affidamenti di incarichi a terzi per lo svolgimento di attività difensiva ovvero nell'ipotesi di attività di collaborazione con soggetti estranei allo Studio, si provvederà a richiedere a costoro di trattare i dati loro affidati ovvero da loro reperiti in conformità a quanto prescritto dal d. l.vo n.196/03 con divieto assoluto di uso improprio dei dati da loro trattati e relativa distruzione dei dati una volta terminato l'incarico affidato.

ALTRE MISURE ADOTTATE

E' stato disposto l'obbligo di provvedere ad un backup settimanale dei dati e dei sistemi installati sul server su cd rom, i quali vengono conservati e chiusi in un cassetto dotato di una chiave, e si è data disposizione di verificare, effettuato il backup, la leggibilità del supporto e che una volta a settimana si proceda a verifica a campione della leggibilità dei dati; custode di detti backup è stato nominato l'incaricato ……
Si è data disposizione che, effettuato un backup, venga distrutto fisicamente il c.d. precedente.
Si è data disposizione che nell'ipotesi di backup o di archiviazione su floppy o supporti riscrivibili si proceda alla formattazione dei supporti prima di procedere ad una riscrittura dei dati.
Si è data disposizione che, terminata la trattazione di una pratica, ogni relativo file, o dato, esistente sui computer, sia cancellato. Per tutti i dati che devono essere conservati per motivi fiscali ovvero, su autorizzazione del cliente per motivi storici e statistici, è stata data disposizione che i dati siano trasferiti su supporti custoditi in un cassetto chiuso a chiave.
Per gli strumenti elettronici,sono state adottate dallo studio le misure di sicurezza, tendenti a ridurre il rischio gravante sui dati e derivante dalla gestione di detti strumenti.
Si è prevista la conservazione in un cassetto chiuso a chiave dei dischi di installazione dei programmi software adottati.
Quanto all'integrità hardware degli strumenti elettronici si è provveduto a stipulare contratto di assistenza con la ditta……che ha rilasciato attestato di conformità del sistema informatico dello Studio alle norme costituenti misure minime ai sensi dell'art. 34 d. l.vo 196/03
Si è data istruzione di cancellazione dei dati una volta esaurito l'incarico ricevuto dal cliente, eccezion fatta per quelli necessari in adempimento di un obbligo di legge (fiscale ed altro)

Sarà adottata ogni altra misura che dal tecnico della manutenzione e dagli sviluppi tecnologici venisse ritenuta utile e necessaria per migliorare la sicurezza degli strumenti elettronici per garantire una maggiore sicurezza dei supporti cartacei.

ATTESTAZIONE

Si attesta che il presente documento è stato redatto in data …… ed è stato sottoscritto in qualità di titolare del trattamento ed è custodito nella cassaforte dello Studio e verrà periodicamente aggiornato al variare delle condizioni ivi contenute.
Il presente documento verrà esibito in caso di controllo.
Il presente documento è stato consegnato in copia a tutti gli incaricati dello Studio dopo esauriente spiegazione.

Andria, lì

Il titolare
Modello predisposto dall'avv. Francesco Tedeschi
Foro di Trani

Modello suggerito da CNF

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ex Art. 34 lett. (g), e n.19.01-08 allegato B.
D.Lgs 30 giugno 2003, n. 196 Codice della protezione dei dati personali

1) Il sottoscritto .....……..... Nato a…….....……. residente in …… (C.F……..), iscritto all'Ordine degli Avvocati di ..... sin dal .....con il n.....nella qualità di Titolare / Responsabile del Trattamento dei dati dello Studio Legale….....…….....con sede in …… …….( ). via…….....n……;

dichiara che:

2) nello Studio Legale vengono trattati i dati personali, sensibili e giudiziari dei:

clienti □	terzi □	(specificare altri eventuali soggetti)……

relativamente a ciò che è strettamente necessario all'espletamento degli incarichi professionali;

collaboratori □	domiciliatari □	fornitori □	(specificare altri eventuali soggetti)…… □

per l'adempimento degli obblighi contrattuali, contabili, tributari e fiscali;

dipendenti □	(specificare altri eventuali soggetti) …… □

per ciò che è necessario all'adempimento degli obblighi di legge in materia di lavoro dipendente e quant'altro

riguardi il rapporto di lavoro.

Il trattamento dei dati dei soggetti sopra indicati riguarda qualunque operazione, o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, necessarie agli scopi sopra specificati, concernenti:

la raccolta □	la registrazione □	l'organizzazione □	la conservazione □
la consultazione □	l'elaborazione □	la modificazione □	la selezione □
l'estrazione □	il raffronto □	l'utilizzo □	l'interconnessione □
il blocco □	la comunicazione □	la cancellazione □	la distruzione di dati □
(specificare eventuali altri tipi di trattamento) …… □			

3) Nello Studio Legale Operano :
a) Avv…….. – Titolare/Responsabile del Trattamento

(Per i dati riguardanti i suoi clienti, i fornitori e il personale collaboratore e di servizio [aggiungere altro se necessario] ...., tratta i dati per tutte le incombenze e le necessità richieste per l'esercizio della professione nel rispetto del Codice per la protezione dei dati personali, del Codice deontologico e della Legge Professionale).

b) Dott…….. - Incaricato del Trattamento

(Nella sua qualità di praticante, è incaricato del trattamento relativamente alle funzioni che derivano per obblighi di legge,
di contratto, e deontologici).

c) Sig……- Incaricata/o Addetta/o al Trattamento .
(Nella sua qualità di operatore amm.vo, segretario/a collaboratore per l'espletamento delle funzioni che gliene derivano per obbligo di legge e di contratto, compresi gli obblighi ad essa/o estesi in ragione della segretezza e della riservatezza sulle informazioni di cui viene a conoscenza).

d) Specificare altri soggetti:

Commercialista □	
Sostituto processuale □	
Consulente tecnico □	
(altro tipo, specificare)..... □	

4)I dati sono trattati mediante inserimento in archivio:

Cartaceo □	Informatico □	(altro tipo, specificare)..... □

a) l'archivio cartaceo è ubicato in
.....
lontano dalla zona dove sostano i clienti e, comunque, inaccessibile a soggetti estranei allo studio;
in particolare all'archivio accedono:
– ....., nella sua qualità di.....
per l'espletamento delle sue funzioni.....

– ....., nella sua qualità di.....
per l'espletamento delle sue funzioni.....

– (specificare eventuali altri soggetti, ruolo e funzioni) ……
……
b) l'archivio informatico è conservato su supporto protetto da credenziali di autenticazione distribuite dal titolare/responsabile del trattamento agli incaricati; a questi ultimi è distribuita anche chiave di accesso al terminale dal quale operano nel rispetto delle disposizioni di cui all'allegato b del T.U.;

(Altro) ……

c) Il sistema informatico è così composto:

N. ……. computer singoli □	N°. …….. computer in rete LAN □
Rete collegata ad internet □	N°. …… computer singoli collegati ad internet □
Dispositivi wireless □	Firewall □ hardware □ software □
Anti-virus □	(Altro) ……□
(Altro)……	
……	

5) Misure di sicurezza adottate:

Oltre alle credenziali di autenticazione per l'accesso agli archivi e alla parola chiave per l'accesso al singolo pc, tutti i computer sono protetti da programmi anti-virus e anti intrusione, periodicamente aggiornati nel rispetto della legge, così come nel rispetto della legge sono periodicamente aggiornati i sistemi operativi;

il portone di ingresso allo Studio è dotato di :

Serratura normale □	Serratura di sicurezza □	Blindatura □
Lo studio è protetto da sistema di allarme.(specificare il tipo)..... □		
Lo studio è protetto da sistema antincendio ..... □		
Contratto con società privata di sorveglianza ..... □		
Impianto elettrico a norma CE ..... □		
Gruppo di continuità per garantire il sistema informatico e quello antifurto ..... □		
Cassaforte ignifuga per conservazione copie informatiche di sicurezza archivi ..... □		
(indicare altri eventuali dispositivi) …… □		
....		

6) Esame dei rischi cui sono sottoposti i dati:
Considerato quanto sopra esposto, tenuto conto dei rischi cui vanno incontro i dati trattati nello studio: furto, incendio, distruzione, accesso abusivo, divulgazione involontaria e volontaria, azione di virus, di worms, blocco del sistema informatico, sottrazione credenziali, distrazione, errori materiali;

(altri eventuali rischi)……

possiamo ragionevolmente dichiarare che tali rischi, sono tutti bilanciati e contrastati dalle misure di sicurezza sopra indicate e adottate in conformità alla normativa in vigore.

(indicare eventuali situazioni diverse da quelle descritte)……
.....

Ogni settimana vengono effettuata copia di backup dei dati informatici per l'accesso alle quali vengono utilizzate credenziali di autenticazione conosciute dal Titolare del trattamento. Le copie di backup sono conservate in luogo sicuro e protetto, diverso da quello in cui vengono abitualmente tenuti i dati; luogo la cui accessibilità è riservata al solo Titolare / Responsabile del trattamento. In caso di perdita totale o parziale dei dati degli archivi, gli stessi possono essere comunque agevolmente ricostruiti e resi disponibili ricorrendo alla copia di back-up.

(altro)……
.....

7) Il Titolare/Responsabile provvede a fornire agli incaricati e agli altri soggetti dello studio, la necessaria formazione sul corretto comportamento necessario al rispetto della legge sulla tutela dei dati personali; oltre a controllare e vigilare sul rispetto delle misure di sicurezza.
8) Nello Studio non si affidano dati all'esterno; qualora però questo sia necessario, per le ragioni del proprio ufficio e professionali, saranno prese le seguenti precauzioni: trasmissione mediante plichi assicurati raccomandati, oppure mediante corriere di fiducia; trasporto in contenitori protetti e sotto il controllo, fino a destinazione, di un incaricato ad acta, in ogni caso per tutti i documenti che usciranno a tali fini dallo studio,

saranno predisposte copie cartacee o informatiche così da poterli ricostruire nei termini previsti dalla norma in caso di sinistro.

(altro)……

……

9) Il DPS così redatto integra e sostituisce il precedente. Si dichiara che il precedente DPS viene distrutto per ragioni di sicurezza contestualmente alla firma del presente documento (dichiarazione volontaria *non obbligatoria per legge).*
Data……..... Avv……

Il presente Dps è da considerare un modello base da integrare e modificare in ragione delle diverse esigenze e realtà che caratterizzano ogni studio legale. Si consiglia di visitare il sito www.garanteprivacy.it

Note di ausilio alla compilazione del documento Programmatico sulla Sicurezza

Punto 1) inserire i dati richiesti corrispondenti all'avvocato che è il dominus dello studio e che è anche il titolare ed eventualmente responsabile del trattamento dei dati . (quest'ultima ipotesi ricorre nel caso in cui non vi siano altri soggetti nominati responsabili del trattamento)

Punto 2) Spuntare le voci relative ai soggetti i cui dati vengono trattati nello studio legale. Qualora venissero trattati dati di soggetti non presenti nell'elenco, specificare gli stessi nella apposita area tratteggiata.

Spuntare i tipi di trattamento effettuati, in genere lo studio legale effettua tutti i trattamenti indicati.

Punto 3) Indicare :
a) Titolare del trattamento (di solito l'avvocato indicato al punto 1).

b) Incaricato del trattamento (generalmente il collaboratore o il praticante).

c) Segretaria/o ed altri soggetti che per ragione del proprio ruolo e funzione all'interno dello studio, accedono ai dati e li trattano.

d) Altri soggetti interni o esterni alla struttura. (Specificare il loro ruolo, i dati da loro trattati e i motivi e le modalità del trattamento, ad esempio il commercialista per i dati da lui trattati ai fini dell'espletamento del mandato professionale, contabili, fiscali, tributari, realtivi al rapporto di lavoro dipendenti e sanitari dei dipendenti stessi; l'eventuale sostituto processuale, il consulente tecnico o di altra natura...ecc...)

Punto 4) Specificare la natura dell'archivio in cui vengono inseriti i dati spuntando la casella relativa;

a) indicare l'ubicazione dell'archivio cartaceo nell'ambito dello dello studio (es : stanza dell'avvocato Tizio o stanza della segretaria ecc...)
indicare poi nome e cognome, qualità (responsabile/incaricato) e funzioni(collaboratore, praticante, segretaria/o).

b) Indicare altri eventuali soggetti indicando sempre la qualità e le funzioni, volendo si può anche indicare dove si trovano materialmente i dati informatici, ad esempio P.C. dell' avvocato, della segreteria, del collaboratore/i nel server della rete Lan...ecc.....

c) Spuntare le caselle interessate indicando anche il numero dei computer presenti ed eventuali altri dispositivi non indicati (ad es: agende elettroniche o telefonini con agenda ed altri strumenti nei quali vengono inseriti i dati).
Per rete LAN si intende una rete composta da computer collegati tra di loro ma non ad internet.

Punto 5)

indicare negli spazi tratteggiati eventuali altri dispositivi di sicurezza non indicati;
spuntare i dispositivi di sicurezza indicati presenti nello studio.

Punto 6) L'esame dei rischi consiste in una ricognizione e successiva valutazione comparata della realtà dello studio legale vista dal punto di vista dei dati trattai, dei rischi cui i dati sono soggetti e delle misure adottate per contrastare adeguatamente questi rischi. Qualora vi siano rischi che non sono adeguatamente contrastati, indicare il modo in cui si intende intervenire per porre rimedio alla situazione di pericolo ed i tempi di intervento.

Punto 7-8) Sono dichiarazioni necessarie e richieste dalla legge, se comunque la realtà dello studio è diversa, sbarrare lo stampato e descriverla.

Punto 9) La dichiarazione è facoltativa, viene resa a seconda le policy sulla sicurezza adottate in precedenza.

CHECK LIST DEI PRINCIPALI ADEMPIMENTI

N.	Adempimenti	Si	No	Osservazioni e memorandum
1	Individuazione dei dati trattati e delle modalità di trattamento.			
2	Informativa e consenso.			
3	Fissazione organigramma e mansionario per incaricato.			
4	Individuazione degli strumenti a disposizione dello Studio per il trattamento dei dati.			
5	Attribuzione delle credenziali di autenticazione (user id e password) ed i profili di autorizzazione.			
6	Predisposizione registro password.			
7	Attribuzione della password composta da 8 caratteri alfanumerici.			
8	Aggiornamento della password.			
9	Disattivazione credenziali non utilizzate.			
10	Attivazione salvaschermo con parola chiave.			
11	Previsione di una password-passepartout.			
12	Installazione antivirus.			
13	Installazione firewall.			
14	Predisposizione scadenzario per gli adempimenti periodici di verifica e controllo degli strumenti hardware, dei programmi software, degli antivirus e delle credenziali di autenticazione.			
15	Predisposizione di attività di formazione degli incaricati.			
16	Istruzioni agli incaricati sull'uso dei programmi e sul trattamento dei dati.			
17	Fissazione delle modalità di accesso agli archivi da parte degli incaricati.			
18	Scelta supporto di archiviazione.			
19	Etichettatura dei supporti di archiviazione.			
20	Individuazione dei luoghi di conservazione dei supporti di conservazione (cartacei e magnetici).			
21	Individuazione modalità di conservazione e verifica integrità dei supporti di archiviazione.			
22	Adozione di misure per la conservazione dei fascicoli.			
23	Fissazione delle modalità di uso e conservazione dei fascicoli da parte degli incaricati.			
24	Elaborazione di un prospetto di valutazione dei rischi.			
25	Adozione misure di prevenzione dei rischi di accesso non consentito e/o distruzione dei dati.			
26	Fissazione modalità di distruzione dei dati al momento della cessazione del trattamento.			

27	Individuazione delle misure per la distruzione dei documenti contenenti dati personali o sensibili.			
28	Adozione misure di ripristino dei dati in caso di malfunzionamento.			
28	Redazione Documento Programmatico della Sicurezza e suo aggiornamento periodico.			
29	Stipula contratto di manutenzione software ed hardware.			
30	Predisposizione delle istruzioni ed avvertenze impartite ai terzi.			

TAVOLA DEGLI ADEMPIMENTI
E DELLE RELATIVE SCADENZE PERIODICHE

Nella tavola si sono indicati i termini prescritti dal Codice della Privacy per il trattamento dei dati sensibili.

Adempimenti	Scadenze,verifica ed aggiornamento
Informativa e consenso	**Prima dell'inizio del trattamento**
Misure di sicurezza	**Prima dell'inizio del trattamento. Nella sua prima applicazione entro il 31/03/2006 ovvero entro il 30/06/2006 nel caso di proroga**
Credenziali autenticazione	**Annuale**
Profili di autorizzazione	**Annuale**
Password	**Trimestrale**
Backup	**Settimanale**
Antivirus	**Semestrale (si consiglia un aggiornamento almeno settimanale se si usa i pc per connessioni ad internet)**
Istruzioni agli incaricati	**Annuale ovvero nel caso di aggiornamento dell'hardware e del software**
Documento Programmatico della Sicurezza	**Nella sua prima applicazione entro il 31/03/2006 e successivamente entro il 31 marzo di ogni anno**
Ripristino dati	**Entro una settimana**
Strumenti elettronici e software	**Annuale ovvero con tempestività nel caso di aggiornamenti del programma di sistema**