Cari Colleghi,
salvo proroghe dell'ultima ora, il 31 marzo 2006 scadrà il termine per la redazione del Documento Programmatico sulla Sicurezza ai sensi dell'art. 36 del D.Lgs 196/2003 (Codice in materia di protezione dei dati personali).
Nella speranza di fornirVi un aiuto per la predisposizione dell'atto, abbiamo redatto una bozza di documento, che alleghiamo alla presente in formato editabile.
Come avrete sicuramente già notato, le proposte di elaborazione del DPSS, rinvenibili su siti istituzionali e non, sono molto numerose: lo scopo dell'iniziativa della Camera Civile è quindi quello di metter a disposizione non solo un modello di documento, che ovviamente andrà adattato alle esigenze ed alla realtà di ogni singolo studio essendo redatto in termini generali, ma anche di fornire uno strumento riepilogativo dei principi fondamentali del Codice e degli adempimenti principali.
Al DPSS, che andrà aggiornato entro il 31 marzo di ogni anno, occorrerà dare data certa: il sistema più semplice è quello di far apporre dall'Ufficio Postale un timbro su un francobollo apposto sul documento.
Lo strumento di riferimento per la compilazione del DPSS rimane comunque la guida redatta dal Garante della Privacy e consultabile sul sito www.garanteprivacy.it.
Rammentiamo che in caso di trattamento dei dati con l'ausilio di strumenti elettronici (per chi non lo avesse già fatto secondo la normativa vigente) occorrerà adottare definitivamente le misure minime di sicurezza previste dagli artt. 33 e 34 del Codice, ovvero, sinteticamente: adozione di credenziali di autenticazione con user-id e password (quest'ultima di almeno otto caratteri o comunque di un numero pari al massimo consentito e da modificare ogni tre mesi), adozione di strumenti elettronici di protezione (antivirus e firewall); conferimento per iscritto di istruzioni agli incaricati del trattamento, adozione di procedure per la custodia di copie di sicurezza, per il ripristino della disponibilità dei dati e dei sistemi.
È invece già in vigore a partire dall'1 gennaio 2004 l'obbligo di rilasciare ai clienti l'informativa di cui all'art. 13 del Codice.

Intestazione Studio Legale

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 36 del D.lgs. 196/03 del Codice in materia di protezione di dati personali)

IL PRESENTE DOCUMENTO E' COMPOSTO DA …… PAGINE COMPRESA LA PRESENTE

SCOPO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Intestazione Studio Legale

In questa sezione dovrà essere spiegato sinteticamente lo scopo per il quale il professionista redige il Documento Programmatico Sulla Sicurezza. E' bene precisare che il documento che si andrà a redigere dovrà fungere anche da manuale e quindi dovrà essere uno strumento utile ad ogni incaricato. Un suggerimento potrebbe essere quello di precisare che il DPSS è redatto per descrivere le modalità con cui i dati vengono trattati, organizzati e gestiti dallo studio.

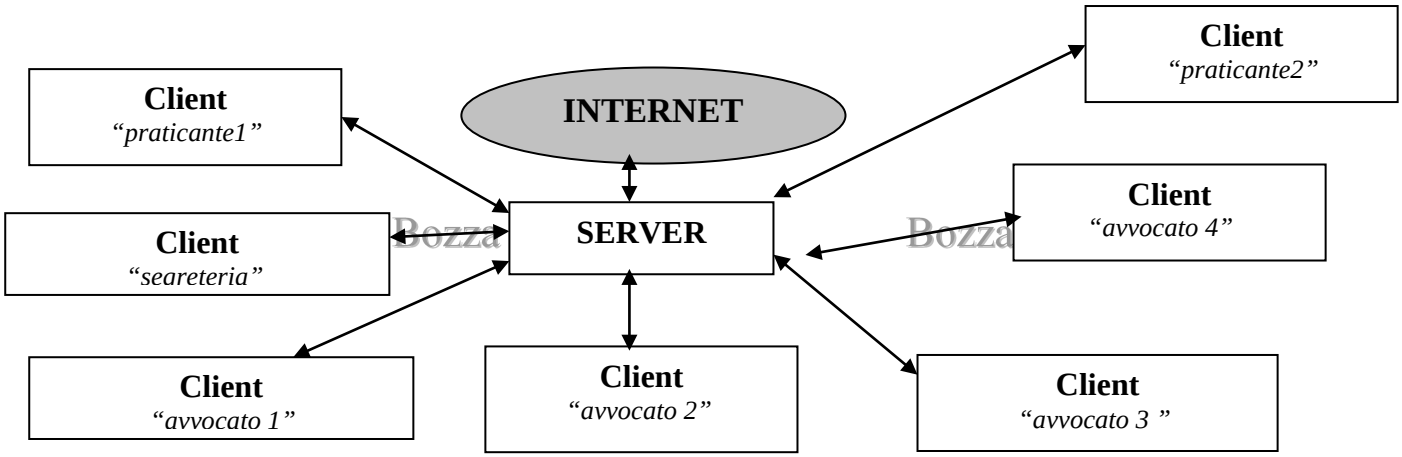
All'interno di questa sezione si potrebbero altresì elencare le autorizzazioni del garante relative al trattamento di determinate tipologie di dati che fanno sì che il professionista non sia obbligato alla loro notifica al garante stesso. In particolare, per quanto riguarda il trattamento dati effettuato in uno studio legale, si potranno identificare le seguenti autorizzazioni:

- Provvedimento Garante per la Protezione dei Dati Personali 21.12.2005 – autorizzazione n. 1, G.U. 03/01/2006, che autorizza il trattamento dei dati sensibili di cui all'art. 4, comma 1, lett. d) del Codice, finalizzato alla gestione dei rapporti di lavoro.
- Provvedimento Garante per la Protezione dei Dati Personali 21.12.2005 – autorizzazione n. 4, G.U. 03/01/2006, che autorizza i liberi professionisti iscritti in albi a trattare i dati sensibili di cui all'art. 4, comma 1, lett. d) del Codice.
- Provvedimento Garante per la Protezione dei Dati Personali 21.12.2005 – autorizzazione n. 7, G.U. 03/01/2006, che autorizza il trattamento di dati di carattere giudiziario. In particolare al capo III lett. b), si precisa che l'autorizzazione al trattamento di dati giudiziari è rilasciata, anche senza richiesta, ai soggetti iscritti nei corrispondenti albi o elenchi speciali, recante l'ordinamento della professione di avvocato.

Intestazione Studio Legale

Inquadramento strutturale ed organizzativo del sistema di trattamento dati

Nella redazione del documento si potrebbe prevedere questa sezione al fine di fare una breve ma esaustiva descrizione dell'organizzazione strutturale ed organizzativa dello studio in relazione al trattamento dati. In particolare si potrebbe prevedere una descrizione della struttura della rete di studio per quanto riguarda il trattamento dati effettuato con strumenti elettronici (elaboratori) e, a seguire, una breve descrizione del trattamento dei dati effettuato con strumenti non elettronici (archivi cartacei). Si potrebbe altresì schematizzare la struttura della rete di studio. Un possibile schema della rete di studio potrebbe essere il seguente:



ELENCO DEI DATI TRATTATI DALLO STUDIO E MODALITA' DI TRATTAMENTO

Intestazione Studio Legale

Nella stesura del documento è importante fare un'attenta analisi dei dati trattati dallo studio (secondo l'attività professionale di ciascuno) e, per ciascuna tipologia di dato, indicare la modalità di trattamento. Dopo aver fatto un elenco di tutti i dati trattati, si indicherà se il trattamento avviene mediante strumenti elettronici o meno, o con entrambi.

Alcune tipologie di dati trattati in uno studio legale potrebbero essere, a titolo esemplificativo, le seguenti:

- *Dati comuni dei clienti ricavabili da elenchi pubblici, visure camerali, trattati con strumenti automatizzati e non;*
- *Dati comuni dei fornitori ricavabili da elenchi pubblici, visure camerali, trattati con strumenti automatizzati e non;*
- *Dati comuni di terzi ricavabili da albi, elenchi pubblici, visure camerali, trattati con strumenti automatizzati e non;*
- *Dati comuni del personale dipendente, trattati con strumenti automatizzati e non;*
- *Dati comuni di altri avvocati e professionisti, trattati con strumenti automatizzati e non;*
- *Dati sensibili del personale dipendente, relativi ai rapporti con gli enti previdenziali ed assistenziali, trattati con strumenti automatizzati e non;*
- *Dati giudiziari dei clienti idonei a rivelare i provvedimenti di cui all'art. 3 DPR 313/2002, o idonei a rivelare la qualità di imputato o indagato, trattati con strumenti automatizzati e non;*
- *Dati giudiziari di terzi idonei a rivelare i provvedimenti di cui all'art. 3 DPR 313/2002, o quelli idonei a rivelare la qualità di imputato o indagato, trattati con strumenti automatizzati e non;*
- *Dati sensibili dei clienti dagli stessi forniti per l'espletamento dell'incarico conferito allo studio, in particolare quelli idonei a*

rivelare l'origine razziale ed etnica, le convinzioni o l'adesione a organizzazioni di carattere religioso, politico, sindacale o filosofico, trattati con strumenti automatizzati e non;

- *Dati sensibili dei clienti forniti dagli stessi per l'espletamento dell'incarico conferito allo studio, idonei a rivelare lo stato di salute, trattati con strumenti automatizzati e non;*
- *Dati sensibili di clienti o di terzi relativi alla sfera sessuale, trattati con strumenti automatizzati e non;*
- *…….*

Figure del trattamento e relativi compiti

Si potrebbe poi passare ad una descrizione delle figure del trattamento dati, così come previste dal Codice in materia di trattamento dei dati personali.

Si potrebbe ad esempio, per ogni figura individuata all'interno della propria struttura, oltre che fare una descrizione delle funzioni e dei compiti di competenza di tale figura, indicare il nominativo della persona a cui tale funzione è assegnata.

Nella struttura di uno studio legale si potrebbero individuare le seguenti figure coinvolte nel trattamento:

- Titolare e/o responsabile del trattamento (che potrebbero, in studio di medie/piccole dimensioni, coincidere). Elencare tutte le funzioni assegnate a tale figura (ad esempio il titolare nomina tutti gli incaricati al trattamento dati e fornisce loro tutte le istruzioni necessarie; adotta tutte le misure necessarie per ridurre al minimo il rischio di perdita/distruzione dei dati; redige ed aggiorna ad ogni variazione l'elenco dei sistemi di

elaborazione connessi in rete; attribuisce, anche con l'ausilio del custode delle password, se nominato, una parola chiave a ciascun incaricato per l'utilizzazione dell'elaboratore; annualmente verificherà la sussistenza delle specifiche che consentivano ad un incaricato di trattare o meno una data categoria di dati e le modalità di trattamento….). Ovviamente in presenza di titolari e responsabili non coincidenti in un'unica figura, le funzioni sopra indicate dovranno essere ripartite tra gli stessi.

- *NB: parte delle funzioni sopra descritte possono identificare il titolare e/o responsabile anche come <u>amministratore del sistema informatico</u>*

- <u>Incaricati del trattamento.</u> In questa sezione dovranno essere indicati tutti i soggetti facenti parte dello studio che vengono incaricati di trattare i dati dal titolare (gli incaricati al trattamento in uno studio possono essere: le segretarie, i praticanti, i collaboratori). Per ogni incaricato dovranno essere individuati i tipi di dati e le relative specifiche di trattamento al quale lo stesso è autorizzato. Pertanto per ognuno andrà indicato, per ciascuna tipologia di dato, il trattamento che è consentito a tale soggetto. Di seguito si riporta un esempio:
  - L'incaricata [nome, cognome], segretaria di studio, è autorizzata dal titolare del trattamento a trattare i seguenti dati : dati personali dei clienti/fornitori, dati sensibili dei clienti/fornitori…. La stessa dovrà attenersi alle istruzioni che le sono state impartite dal titolare mediante lettera di incarico e dovrà comunque rispettare le "norme generali di prevenzione" che di seguito si riportano :

- *I dati personali devono essere trattati secondo i principi indicati dalla legge (ogni qualvolta fosse necessario, l'incaricato dovrà visionare il testo del D. Lgs 196/03, che è messo a disposizione di tutti);*
- *Verificare la pertinenza e non eccedenza dei dati trattati rispetto alle finalità della raccolta;*
- *Controllare l'esattezza dei dati ed eventualmente, qualora si renda necessario, provvedere al loro aggiornamento;*
- *Conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi della raccolta o alla custodia dei documenti per legge(archivio legale); superato tale termine provvedere alla cancellazione del dato (o alla sua trasformazione in forma anonima);*
- *Rendere ai soggetti interessati l'informativa di cui all'art. 13;*
- *Acquisire sempre il consenso scritto per il trattamento dei dati dell'interessato, in particolar modo per i dati sensibili. La nomina di ciascun incaricato deve essere fatta per iscritto. La lettera di nomina dovrà essere fatta firmare all'incaricato per accettazione e presa visione di tutte le specifiche in essa contenute e alle quali dovrà attenersi nello svolgimento delle proprie mansioni; una copia della lettera dovrà essere consegnata all'incaricato.*

A discrezione del titolare i compiti di seguito elencati *a titolo esemplificativo*, potranno essere affidati ad uno o più incaricati.

- Il Custode delle Password. Il custode delle password è nominato dal titolare del trattamento. Tale figura può essere scelta anche fra i soggetti incaricati al trattamento. Anche questa nomina deve avvenire per iscritto, tramite lettera consegnata in copia al designato. L'originale deve essere fatto sottoscrivere per ricevuta e conservato a cura del titolare del trattamento. Tale nomina è a tempo indeterminato e viene meno per revoca o dimissione del custode delle password. E' compito del custode delle password:
  - *predisporre le password per ogni incaricato (confronta schema pag. 3);*
  - *creare nuove password per ogni incaricato con cadenza almeno trimestrale, annullando tutte le precedenti (le password sono individuali e non riutilizzabili);*
  - *revocare e/o annullare tutte le password rimaste inutilizzate per un periodo superiore a sei mesi;*
  - *creare nuove password nel caso di guasto ai sistemi operativi che comportino un'intervento da parte del personale tecnico addetto all'assistenza;*
  - *non rivelare a nessun soggetto estraneo al trattamento le password assegnate a ciascun incaricato e custodire le medesime in luogo sicuro.*
- L'incaricato alle copie di backup. Il titolare del trattamento nomina un addetto alle copie di backup. La nomina è effettuata sempre per iscritto a mezzo lettera consegnata direttamente al soggetto designato, il quale dovrà controfirmarla per ricevuta ed

accettazione dell'incarico. *All'addetto alle copie di backup saranno consegnate tutte le istruzioni necessarie allo svolgimento del compito affidatogli. Copia della lettera di incarico e le relative istruzioni dovrà essere conservata a cura del titolare del trattamento*

> **Suggerimento**: *In linea generale il backup dei dati dovrebbe essere effettuato con cadenza almeno settimanale tramite l'utilizzo di idonei supporti, fissi o removibili, e di capacità idonea a supportare una pluralità di backup nel tempo, che dovranno essere consegnati al titolare del trattamento, il quale li custodirà in luogo sicuro.*

- L'incaricato alla gestione dell'Antivirus. Il titolare del trattamento affida ad un incaricato il compito di eseguire le periodiche scansioni antivirus e gestire il programma stesso. Anche in questo caso la nomina avviene per iscritto e consegnata direttamente al designato e controfirmata dallo stesso per ricevuta ed accettazione dell'incarico. *Unitamente alla lettera di incarico dovranno essere consegnate all'incaricato anche tutte le istruzioni necessarie allo svolgimento del compito affidatogli. In particolare è compito dell'addetto alla gestione dell'antivirus aggiornare il programma stesso almeno con cadenza trimestrale (qualora non siano già previsti aggiornamenti automatici più frequenti, ad esempio in presenza di nuove definizioni di virus), verificare l'efficienza dello stesso ed effettuare con cadenza almeno settimanale le scansioni antivirus su tutta la rete di studio, e creare, se necessario, un documento riepilogativo delle scansioni effettuate. Ad ogni buon conto, in caso di una gestione automatizzata degli aggiornamenti, l'incaricato della gestione dell'Antivirus, dovrà verificare che ciò avvenga correttamente, ed agire manualmente*

qualora insorgessero problemi con l'aggiornamento e con le scansioni programmate.

In calce a questa sezione sarà opportuno riepilogare i soggetti (titolare e incaricati) e i rispettivi ruoli.

Titolari e incaricati al trattamento dati

- I titolari del trattamento sono (in caso di studi associati ciascun professionista):
  - Avvocato …….

- L'amministratore del sistema informatico è:
  - Avvocato ……

- Gli incaricati del trattamento sono:
  - …… (collaboratore di studio)
  - …….. (segretaria di studio)
  - ……..(praticante)
  - ……. (praticante)
  - ……

- Il custode delle password è:
  - …….
- L'incaricato alle copie di backup è:
  - ……
- L'incaricato alla gestione dell'antivirus è:
  - …….

DISPOSITIVI ANTI-INTRUSIONE, STRUMENTI AUTOMATIZZATI E NON

Intestazione Studio Legale

In questa sezione, premessa una identificazione dell'ubicazione dello studio (e delle eventuali sede secondarie), si potrà fornire una descrizione degli uffici con riferimento a tutti quei dispositivi che hanno attinenza con la sicurezza (eventuali allarmi, sistemi di videosorveglianza, protezione dei serramenti dalle intrusioni….), nonché tutte quelle apparecchiature che garantiscono il funzionamento dell'ufficio, tanto quelle automatizzate (stampanti, fax, telefoni, computer e quant'altro), quanto quelle non automatizzate (archivi cartacei).

Il tutto andrà compilato in modo il più possibile analitico, in forma di inventario.

Ad esempio:

- *Nr. 1 computer connesso in rete, marca ……., con collegamento ad Internet (se presente) , posto nel locale……, utilizzato dall'incaricato……con sistema operativo……..;*
- *……*

In calce all'elenco sarebbe opportuno indicare i soggetti incaricati della manutenzione delle varie apparecchiature presenti nell'ufficio, ciascuno secondo la propria competenza.

SISTEMI OPERATIVI E APPLICAZIONI UTILIZZATE DALLO STUDIO

Intestazione Studio Legale

In questa sezione si dovranno indicare i vari sistemi operativi informatici utilizzati sui computer, con riferimento anche a tutti i programmi e le applicazioni adottati per le singole funzioni (videoscrittura, posta elettronica, browser, eventuali programmi di contabilità e software di utilità in genere).

Suggerimento: *sarà compito dell'amministratore del sistema informatico verificare l'autenticità e l'aggiornamento delle licenze d'uso.*

AMBITO DI TRATTAMENTO DEGLI INCARICATI IN BASE ALLE DIVERSE TIPOLOGIE DI DATI E RILEVAZIONE DEL RISCHIO CONNESSO AL TRATTAMENTO STESSO

In questa sezione si descriveranno, con maggiore precisione rispetto alle indicazioni fornite nelle sezioni precedenti, tutti i dati comunque trattati e tutti i soggetti autorizzati al loro trattamento.

A titolo esemplificativo si indicheranno:

- *I dati comuni dei clienti, dei fornitori o dei terzi, i dati comuni di altri avvocati e professionisti cui lo studio affida incarichi o si rivolge per consulenze, i dati giudiziari dei clienti, quelli di terzi, i dati sensibili dei clienti e dei terzi, sono trattati, per esigenze connesse al tipo di attività svolta, oltre che dai titolari del trattamento, anche dagli incaricati;*
- ……;

Successivamente si dovrà presentare un'analisi dei rischi connaturati ai dati sopra indicati.

Sempre a titolo esemplificativo si descrive un'ipotesi di analisi, che tuttavia ciascun professionista dovrà rideterminare in funzione della propria struttura e delle condizioni effettive riscontrabili:

- *Per i dati comuni del personale dipendente (quelli necessari al rapporto di lavoro, alla reperibilità e corrispondenza con gli stessi, e inerenti i rapporti fiscali), i dati comuni dei clienti (dagli stessi forniti per l'espletamento del mandato conferito, compresi quelli relativi al patrimonio e alla situazione economica o necessari per disposizioni fiscali o quelli relativi alla reperibilità e corrispondenza con gli stessi), i dati comuni di terzi (forniti dai clienti stessi, compresi i dati relativi al patrimonio ed alla situazione economica o necessari alla reperibilità e corrispondenza con gli stessi o per atti giudiziari), i dati comuni dei fornitori (concernenti la reperibilità e la corrispondenza con gli stessi, nonché quelli relativi ai rapporti fiscali), i dati comuni di altri avvocati o professionisti cui lo studio affida incarichi ed i dati comuni dei clienti, dei fornitori, dei terzi o di altri professionisti ricavabili da albi, elenchi pubblici, visure camerali, sia in relazione alla loro natura, sia al nostro tipo di struttura, il rischio connesso alla loro gestione è da definirsi …….., in quanto lo studio utilizza ……;*
- *Per i dati sensibili del personale dipendente, i dati giudiziari dei clienti, dei terzi, i dati sensibili forniti dai clienti, i dati sensibili di terzi (forniti dai clienti al fine dell'espletamento del mandato conferito), il rischio della loro gestione è da definirsi ……., fatta eccezione per quei dati idonei a rivelare lo stato di salute, o dati giudiziari di clienti o terzi e le pratiche quali quelle in materia di diritto familiare con dati idonei a rivelare la vita sessuale, per la loro natura il rischio è da ritenersi ……. Possiamo comunque dire che in relazione al tipo di struttura, tale rischio si può ritenere ……, in quanto lo studio utilizza ……...*

Inoltre si dovrà presentare un'analisi dei rischi connessi al trattamento dei dati mediante l'utilizzo di strumenti automatizzati e non.

Sempre a titolo esemplificativo si descrive un'ipotesi di analisi, che tuttavia ciascun professionista dovrà rideterminare in funzione della propria struttura e delle condizioni effettive riscontrabili:

- *Relativamente alle apparecchiature hardware i rischi cui possiamo incorrere sono principalmente quelli derivanti dal malfunzionamento degli elaboratori o dovuti ad eventi naturali (ad es. temporali con conseguenti guasti al sistema elettrico o telefonico). In questo caso il rischio è da considerarsi di …… entità, avendo lo studio adottato tutte le misure minime di sicurezza relative, quali ……..;*
- *Relativamente ai software si possono verificare dei problemi dipendenti ad esempio da attacchi da virus, malware, dialer, oppure da un errato uso dei software da parte degli incaricati, o ancora utilizzo di vecchie versioni di software. In tutti questi casi il rischio è da considerarsi di ……. entità, in quanto lo studio ha …….;*
- *Relativamente ai locali in cui i dati sono trattati il rischio rilevato è quello relativo all'accesso all'interno degli stessi da parte di terzi non autorizzati o anche quello connesso all'evento naturale. Nel primo caso il rischio è da definirsi di …….. entità, in quanto ……. Quanto al secondo caso non si può ovviamente valutare con precisione l'entità del rischio, in quanto, del tutto indipendente dalla volontà umana, ma in relazione all'area geografica in cui ci troviamo possiamo valutarlo ……;*
- *Relativamente al rischio connesso all'archivio cartaceo, anche qui lo stesso è da definirsi ……in quanto ……..;*

- *Per quanto riguarda il rischio inerente la riservatezza, lo stesso è da definirsi …., in quanto tutti gli incaricati del trattamento sono stati informati e preparati circa tutte le procedure da seguire al fine di un corretto trattamento dei dati secondo i principi di legge, mentre è inteso che per quanto riguarda i titolari, ossia gli avvocati dello studio, vige il principio del segreto professionale;*
- *……..*

Di seguito si riassumono in una semplice tabella (a titolo esemplificativo e non esaustivo) le diverse tipologie di rischio, indicando la loro entità, in relazione alla struttura ed organizzazione dell'ufficio, e/o ad altri fattori.

Tipologia di Rischio	***Bassa***	***Media***	***Alta***
Fattori ambientali			
Fulmine			
Interruzione di corrente			
Terremoto			
Inondazione			
Fattori tecnici			
Guasto hardware			
Deterioramento dei supporti di memoria			
Danno volontario provocato da terzi estranei			
Guasto tecnico di provider di rete			
Danni sulle linee			
Sovraccarico di traffico			
Guasto software			
Guasto dei servizi di comunicazione			
Evoluzione tecnologica che rende obsoleti i supporti informatici			
Deterioramento nel tempo dei supporti informatici e/o cartacei			
Fattore umano			
Polvere			

Uso non autorizzato dei supporti di memoria			
Errore del personale operativo			
Errore di manutenzione			
Furto			
Accesso non autorizzato alla rete			
Uso della rete in modo non autorizzato			
Uso non corretto delle risorse			
Scarimento di virus e/o dialer per mezzo di posta elettronica e/o operazioni di dowload			
Uso di software da parte di utenti non autorizzati			

MISURE DI SICUREZZA ADOTTATE PER RIDURRE IL RISCHIO

In questa sezione andranno individuate tutte le misure adottate dallo studio legale per contenere il rischio connesso al trattamento dei dati.

A titolo informativo, salva la verifica da parte di ciascun professionista, si indicano alcune soluzioni, alcuni standard e alcune procedure, che sarebbe buona norma tenere presente:

- *Raccolta dati attraverso il consenso scritto dell'interessato, mediante sottoscrizione da parte dello stesso di apposito modello che verrà poi consegnato in copia al cliente stesso (informativa art. 13 e formula di consenso al trattamento dei dati sensibili);*
- *Istruzioni scritte agli incaricati del trattamento, e se il titolare lo ritenesse necessario, farà partecipare gli incaricati ad appositi corsi sulla formazione in merito alla privacy*;
- *Sistema di autenticazione informatica, consistente nell'assegnare a ciascun incaricato una user id e una password. User id e password saranno diversificate per ogni utente; la password sarà composta di almeno otto (8) caratteri (o comunque dal numero massimo di caratteri consentiti dal sistema operativo in uso). L'user id sarà l'identificativo dell'utilizzatore dell'elaboratore (nominativo*

dell'incaricato), mentre la password non potrà contenere elementi facilmente ricollegabili al suo utilizzatore. La password è assegnata dal custode delle password personalmente a ciascun incaricato. Ogni tre mesi tutte le password saranno cambiate a cura del custode delle password; le password inutilizzate verranno disattivate e non potranno più essere riutilizzate;

- *Utilizzazione di gruppo di continuità con autonomia di 12 ore nel caso di interruzione momentanea di corrente;*
- *Ogni incaricato è preventivamente informato sulla tipologia di dati sui quali lo stesso potrà effettuare il trattamento, secondo le modalità previste dal titolare.*
- *Chi utilizza personal computer non dovrà mai lasciare incustodito lo stesso, senza prima essersi assicurato di aver chiuso tutte le sessioni di lavoro;*
- *Per ogni messaggio e-mail in entrata deve esserne controllata la provenienza;*
- *Per ogni singolo computer è prevista la funzione di aggiornamento automatico del sistema fornito da….;*
- *Installazione di adeguati e aggiornati software anti-virus;*
- *Previsione di backup dei dati con frequenza alemno settimanale;*
- *Non devono essere lasciati incustoditi sulle scrivanie o altri ripiani, atti, documenti o fascicoli delle pratiche. I fascicoli vanno conservati nell'armadio preposto per la loro custodia e devono essere riposti integri nel loro contenuto al termine delle operazioni di trattamento;*
- *Le comunicazioni a mezzo posta o fax dovranno essere tempestivamente smistate ai vari destinatari e pertanto non dovranno essere lasciate incustodite sulle scrivanie o altri ripiani, con il rischio che terzi non autorizzati al trattamento possano venire a conoscenza del contenuto;*

- *L'armadio contenente i fascicoli relativi alle pratiche di questo studio deve essere chiuso a chiave ad ogni fine giornata lavorativa, così come l'armadio delle pratiche archiviate definitivamente;*
- *I documenti cartacei non utilizzati (quali ad es. fotocopie malriuscite), contenenti dati sensibili, non devono essere riutilizzati come carta per appunti, ma dovranno essere distrutti tramite l'apposito dispositivo distruggi documenti o in alternativa ridotti in piccoli pezzi;*
- *Deframmentazione periodica dei dischi rigidi;*
- *Aggiornamento periodico dell'ambito di trattamento consentito ai singoli incaricati;*
- *Inventario dei sistemi di elaborazione con controllo almeno annuale dell'efficienza degli stessi e dell'adeguatezza dei sistemi operativi utilizzati per il trattamento dati;*
- *Nomina del custode delle password;*
- *Garantire l'integrità dei dati trattati attraverso un primo controllo col cliente e successivamente confrontando i dati contenuti sui supporti cartacei con quelli sui supporti informatici;*
- *Garantire la sicurezza delle trasmissioni di dati tramite e-mail, adottando, se necessario, sistemi di cifratura dati;*
- *Assicurarsi che i dati che potrebbero venire trasmessi a soggetti esterni allo studio per ragioni inerenti l'attività svolta, come ad esempio Ufficio Paghe, altri professionisti, banche…, siano pertinenti e non eccedenti al tipo di trattamento che dovrà essere effettuato da questi ultimi e che tali soggetti siano a conoscenza delle procedure di trattamento consentite e comunque previste dalla legge in materia di protezione dei dati personali;*

- *Rilascio di autorizzazioni specifiche ai soggetti esterni alla struttura che devono accedere ai locali dove vengono trattati i dati, come ad esempio l'impresa di pulizie e i tecnici della manutenzione delle macchine elettroniche e della telefonia;*
- *Rinnovo annuale della polizza assicurativa di studio;*
- *Verifiche periodiche dell'efficienza dei sistemi anti-intrusione (portoncino blindato) e di tutti gli strumenti elettronici presenti in studio (cassaforte, sistemi di elaborazione, dispositivo distruggi documenti, fotocopiatrice), nonché dei sistemi di telefonia e di custodia degli archivi cartacei (funzionamento delle serrature degli armadi, dei cassetti);*
- *Al termine della giornata lavorativa assicurarsi che tutte le porte e le finestre vengano chiuse;*
- *Aggiornamento e revisione annuale del Documento Programmatico Sulla Sicurezza.*

Nel caso di trattamento di dati sensibili particolari, quali dati genetici o comunque quelli atti a rivelare lo stato di salute e la vita sessuale di un individuo, oltre alle misure di sicurezza di cui sopra, dovranno essere adottati ulteriori accorgimenti, *che a titolo esemplificativo, potrebbero essere:*

- *Tenere separati questi tipi di dati dagli altri, anche per mezzo di archivio separato;*
- *Applicare una protezione crittografica, se necessario;*
- *Effettuare il collegamento tra questi dati e gli altri per mezzo di un codice comprensibile all'incaricato.*

ISTRUZIONI PARTICOLAREGGIATE PER IL TRATTAMENTO DEI DATI MEDIANTE L'UTILIZZO DI SUPPORTI REMOVIBILI E CON STRUMENTI NON ELETTRONICI

Trattamento dati mediante l'utilizzo di supporti removibili

Individuare ed indicare i diversi supporti utilizzati e successivamente elencare una serie di istruzioni finalizzate al trattamento dei dati per mezzo di tali supporti di cui si fornisce un *elenco esemplificativo.*

L'incaricato dovrà:

- *Accertarsi che il supporto sia vuoto o comunque privo di altri file che potrebbero risultare infetti;*
- *Nel caso di floppy disk effettuare sempre la formattazione dello stesso;*
- *Una volta memorizzati i dati sul supporto, solo ed esclusivamente quelli necessari allo svolgimento del proprio compito, assicurarsi di aver attivato tutte le protezioni contro possibili nuove ed accidentali scritture;*
- *Apporre sempre un etichetta di riconoscimento sul supporto (floppy o CD-RW) in modo da non poterlo confondere con altri;*
- *Il supporto contenente dati sensibili e/o giudiziari deve essere custodito personalmente dall'incaricato che ne ha creato la copia, in luogo adatto e sicuro;*
- *Quando i dati contenuti nel supporto non hanno più ragione di essere devono essere cancellati, il supporto riformattato e l'etichetta rimossa, nel caso di floppy o CD-RW;*
- *Il supporto può essere consegnato ad altro incaricato, purchè abbia lo stesso profilo di autorizzazione;*
- *Fare attenzione al luogo dove il supporto viene custodito (nel caso di floppy o CD-RW, lo stesso dovrà essere tenuto lontano da campi magnetici, fonti di calore…);*
- *Il supporto contenente dati sensibili non deve mai essere lasciato incustodito sul tavolo o nel pc;*

- *Quando i dati dal supporto vengono trasferiti nuovamente sul disco rigido del pc, cancellare l'intero contenuto del supporto.*

Trattamento con strumenti non elettronici

Individuare ed indicare tutti gli strumenti diversi da quelli elettronici utilizzati e successivamente elencare una serie di istruzioni finalizzate al trattamento dei dati per mezzo di tali strumenti, di cui si fornisce un *elenco esemplificativo.*

- *L'asportazione dei documenti dal luogo dove vengono normalmente custoditi dovrà essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento;*
- *Al termine delle operazioni di trattamento i documenti dovranno essere riposti esattamente al loro posto;*
- *L'incaricato che utilizza un determinato fascicolo dovrà assicurarsi che, al momento della restituzione, lo stesso sia completo ed integro, in altre parole che il contenuto alla restituzione sia lo stesso di quello del prelievo;*
- *Se si dovessero lasciare, ad esempio di sera alla fine della giornata lavorativa, fascicoli fuori dall'armadio, l'incaricato dovrà assicurarsi che gli stessi siano in un luogo altrettanto sicuro (ad es. cassetto chiuso a chiave);*
- *In generali i documenti non devono essere lasciati incustoditi sul tavolo;*
- *Accertarsi che terzi individui, estranei alla struttura dello studio, come ad esempio l'addetto alla manutenzione o l'addetto alle pulizie, non possa venire a conoscenza dei contenuti di detti documenti;*
- *Trattare con cautela eventuali documenti consegnati in originale;*

- *Nel caso di spedizione per posta di originali o fotocopie dei documenti, utilizzare principalmente la spedizione tramite raccomandata con ricevuta di ritorno (in casi particolari anche assicurata) o comunque a mezzo corriere;*
- *Eventuali fotocopie non riuscite devono essere distrutte nell'apposito "dispositivo distruggi documenti" o in alternativa devono essere ridotte in pezzi di dimensioni ridotte in modo che non sia possibile ricostruire il documento;*
- *Le fotocopie non riuscite non devono essere usate come carta per appunti, né all'interno dello studio, né tanto meno all'esterno;*
- *Durante il trasporto di documenti fuori dallo studio è necessario che l'incaricato tenga sempre con sé la borsa o la cartella contenente tali documenti, in modo che gli stessi non possano essere visionati da terzi soggetti non autorizzati al trattamento;*
- *Nelle comunicazioni telefoniche accertarsi dell'identità del proprio interlocutore al fine di non divulgare dati a soggetti non autorizzati;*
- ……

PIANO DI RIPRISTINO DELL'IPOTESI DI DANNEGGIAMENTO DEI DATI O DEGLI STRUMENTI ELETTRONICI

In questa sezione si dovranno elencare le istruzioni necessarie allo scopo.

Sempre a titolo esemplificativo:

- *avvertire il titolare del trattamento e l'incaricato che ha in custodia le copie di backup e i cd contenenti i vari software installati;*
- *rivolgersi immediatamente al tecnico manutentore della ditta "…….." al fine di chiedere un intervento, sollecitandone al più presto l'assistenza;*
- *una volta reinstallati tutti i programmi danneggiati, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nel supporto utilizzato per le copie di backup;*
- *provvedere all'immediato aggiornamento dei sistemi operativi una volta reinstallati;*
- *in ogni caso viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro o non oltre 7 giorni;*
- *al fine di evitare il danneggiamento degli strumenti elettronici e dei dati in essi contenuti, si prevede che per due volte all'anno sia effettuata manutenzione in modo adeguato dal tecnico incaricato.*

FORMAZIONE DEGLI INCARICATI

In questa sezione di dovrà descrivere i metodi utilizzati per la formazione di ciascun incaricato.

Ancora a titolo esemplificativo:

"La formazione avviene all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati e comunque con frequenza annuale. Essa tenderà a sensibilizzare gli incaricati sulle tematiche della sicurezza, facendone comprendere i rischi e le rispettive responsabilità (con specifica delle sanzione connesse, sia penali che disciplinari) che riguardano il trattamento dei dati personali. Inoltre la formazione tenderà alla più esauriente possibile spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni del sistema operativo. La formazione è fatta dal titolare dello studio."

CAUTELE IN FASE DI AFFIDAMENTI DI DATI PERSONALI A TERZI SOGGETTI ESTERNI ALLO STUDIO

Ciascun professionista, in relazione alla tipologia di attività esercitata, valuterà le misure da adottare nell'eventualità di trasmissione di dati a terzi estranei allo studio e ne darà descrizione nella presente sezione, curando sempre di ottenere le necessarie autorizzazioni dai soggetti i cui dati vengono trasmessi.

AGGIORNAMENTO PERIODICO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Come previsto dal comma 19 del D. Lgs 196/03 il presente Documento Programmatico Sulla Sicurezza verrà controllato e aggiornato entro il 31 marzo di ogni anno. *Annualmente verranno pertanto verificate le seguenti condizioni (se ne riportano alcune a titolo esemplificativo):*

- *Per quanto riguarda l'accesso fisico ai locali dove si effettua il trattamento verrà in particolare verificata l'efficienza dei sistemi anti-intrusione ;*
- *Per quanto riguarda l'utilizzo di supporti magnetici per la memorizzazione dei dati, si verificherà in particolare:*
  - *Che vengano utilizzati tutti gli accorgimenti necessari per l'utilizzo e la memorizzazione dei dati personali, quindi che:*
    - *vengano utilizzati esclusivamente supporti di tipo riscrivibile;*
    - *vengano memorizzati solo i dati strettamente necessari allo svolgimento di quel particolare trattamento;*
    - *i supporti vengano custoditi in luogo sicuro;*
    - *si provveda alla cancellazione degli stessi quando il trattamento è terminato, e comunque che vengano seguite tutte le istruzioni sopra riportate e più precisamente al paragrafo dedicato alle istruzioni da seguire per il trattamento con supporti removibili;*
- *Relativamente all'efficienza dei sistemi di autenticazione informatica si verificheranno in particolare:*
  - *la conoscenza di ogni incaricato circa i propri profili di autorizzazione, campi di applicazione e utilizzo delle password;*

- *la persistenza dei requisiti di ogni singolo incaricato circa i dati cui gli è stato autorizzato il trattamento e le modalità di trattamento stesse;*
- *le modalità di gestione e rinnovo delle password*

- *Per quanto riguarda le procedure atte a verificare l'integrità e l'aggiornamento dei dati trattati, in particolare si verificherà:*
  - *che le procedure utilizzate per memorizzare un dato cartaceo su supporto magnetico siano adeguate a garantire l'integrità del dato stesso;*
  - *che le copie di backup vengano regolarmente effettuate e secondo le modalità precisate dal titolare del trattamento;*
  - *che gli archivi cartacei vengano gestiti secondo le istruzioni impartite dal titolare del trattamento*
- *Per quanto riguarda le trasmissioni in rete e spedizioni in generale, si verificheranno in particolare:*
  - *L'efficienza delle linee telefoniche e del modem;*
  - *Nell'eventualità di utilizzo di programmi di crittografia, l'efficienza degli stessi;*
  - *Se le modalità di spedizione utilizzate per i documenti cartacei corrispondono a quanto disposto dal titolare del trattamento*
- *Per quanto riguarda le modalità di conservazione dei documenti su supporti non automatizzati, si verificheranno in particolare:*
  - *Se le procedure utilizzate per la conservazione dei dati corrispondono esattamente a quanto disposto dal titolare del trattamento, e pertanto:*
    - *l'effettivo corretto utilizzo degli armadi muniti di serratura;*
    - *l'applicazione di tutti gli accorgimenti necessari nel caso di trasporto fuori studio di documenti;*

- *l'applicazione di tutti gli accorgimenti necessari durante il trattamento dei dati;*
- *la distruzione manuale o per mezzo del "dispositivo distruggi documenti" dei documenti cartacei non più utilizzati per i quali è terminato il trattamento, delle fotocopie mal riuscite…;*
- *l'applicazione di tutte le misure di sicurezza previste dal presente D.P.S.S..*

DICHIARAZIONE D'IMPEGNO E FIRMA

Il presente Documento Programmatico Sulla Sicurezza, redatto in data ……., viene firmato in calce dagli avvocati ……, in qualità di titolari del trattamento, e verrà aggiornato periodicamente entro il 31 marzo di ogni anno, così come previsto dalle vigenti norme in materia di trattamento di dati personali.

Data, ……..

Avvocato……..