

Unione Triveneta Consigli dell'Ordine degli Avvocati

Documento programmatico sulla sicurezza

IL DOCUMENTO espone UN PROGRAMMA cioè cosa si vuole o si deve fare per adeguarsi alla normativa ed evitare i rischi sopra descritti sul trattamento dei dati

Il titolare redige un documento programmatico sulla sicurezza contenente:
la **ricognizione dei dati trattati** e **l'analisi dei rischi** che incombono sui dati

le **misure da 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**

la **descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento**

la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di **dati personali affidati, in conformità al codice, all'esterno** della struttura del titolare

La stesura del **DPS** è una misura minima, da farsi entro il 31 marzo di ogni anno (per la prima volta entro il 30.6.2004).

PER REDIGERE IL DOCUMENTO BISOGNA PERCIO' PORSI 5 DOMANDE:

Quali dati tratto?

*Faccio il **censimento** dei dati, a chi si riferiscono, individuo le **finalità** e **modalità***

Quali rischi li minacciano
*Rischi **Possibili***
*Rischi **Probabili** (poco/molto)*
*Rischi **Prevedibili** (no/sì)*
*Rischi **Prevenibili** (no/sì)*

Quali contromisure?
*Quelle che **ho** adottato*
*Quelle che **mi mancano***

L'ANALISI DI TUTTO CIO' E' IL **DPS** che non puo' essere schematizzato o generalizzato, ma va fatto per ogni singolo caso.

E' opportuno dare **data certa** al DPS.

Quello che segue è un esempio di DPS, contiene delle proposte di lavoro perché non è possibile schematizzare le diverse situazioni di ogni studio legale.

Ipotesi di Modello di Documento programmatico sulla sicurezza nel trattamento dei dati personali

Scopo di questo documento è quello di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dallo Studio Legale

Il presente documento è stato redatto da.....in qualità di titolare/responsabile per la sicurezza, che provvede a firmarlo in calce

Elenco dei trattamenti di dati personali

Lo Studio Legale tratta direttamente o per mezzo di collaborazioni esterne (esempio visuristi, società di servizi, altri Avvocati) i seguenti dati:

dati comuni dei clienti (quali nominativo, indirizzo, codici fiscali, situazioni patrimoniali, certificati anagrafici, dati contabili), dei fornitori o di **terzi ricavati da albi, elenchi pubblici, visure camerali, visure catastali e di Conservatoria;**

dati comuni del personale dipendente (quali nominativo, indirizzo, codici fiscali, certificati anagrafici, dati contabili), quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria;

dati comuni dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;

dati comuni di terzi (quali nominativo, indirizzo, codici fiscali, situazioni patrimoniali, certificati anagrafici, dati contabili), forniti dai clienti per l'espletamento degli incarichi affidati allo studio, 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;

dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria;

dati comuni di altri Avvocati e professionisti (quali nominativo, indirizzo, codici fiscali) cui lo studio affida incarichi o si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti a finalità fiscali o dati di natura bancaria;

dati sensibili del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o l'adesione ad organizzazioni sindacali;

dati giudiziari dei clienti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato;

dati giudiziari di terzi idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato;

dati sensibili dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare l'origine razziale ed etnica, le

convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico;

dati sensibili dei clienti, dagli stessi forniti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;

dati sensibili di terzi, forniti dai clienti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;

dati sensibili di clienti o terzi, comunque afferenti la vita sessuale;

dati genetici di clienti o terzi.

Il trattamento di tali dati è **fatto prevalentemente all'interno dello studio**, dagli avvocati, dai collaboratori e dal personale di segreteria, **per l'attività preparatoria a quelle difensiva, l'attività giudiziale, l'attività di consulenza e l'attività stragiudiziale di cui lo studio viene incaricato, nonché per l'espletamento delle attività amministrative e contabili dello studio.**

Vengono posti in essere i trattamenti di cui all'art. 4 comma 1 lettera A, **eccezion fatta per la diffusione** (salvo specifica richiesta del cliente).

Tutti i dati non pubblici vengono acquisiti previa **informativa**.

Questi dati vengono trattati e conservati in fascicoli riposti in schedari dotati di chiusura, nonché trattati tramite computer in rete in locali protetti e con accesso ad internet, archiviati al termine della pratica. I dati dei clienti sono trattati tramite gli strumenti elettronici con il programma gestionale per studi legali.

Lo studio, ove vengono trattati i dati, è **ubicato** in un condominio in zona, dotato di portone di ingresso a chiusura automatica e con videocitofono, con sorveglianza notturna, e porte blindate; sito al piano..... I **singoli studi (in nr.)**, che lo compongono, sono dotati ciascuno di porta con chiusura a chiave, così come l'archivio. La

segreteria è ubicata in un locale..... **la zona di attesa** per i clienti L'**archivio** si trova

Lo studio è dotato di cassaforte con chiusura a chiave.

Ogni studio è dotato di un computer in rete e connesso ad internet con connessione ADSL in rete; ove è ubicata la segreteria si trovano due **postazioni di lavoro** con computer con connessione ADSL ad internet ed in fianco ad una di esse è ubicato il server connesso ad internet ed il router per la connessione ad internet. Inoltre in questo locale si trovano le stampanti, il fax, la fotocopiatrice e lo scanner. Le linee telefoniche sono due .

Gli strumenti elettronici sono:

nr. 1 computer connesso in rete ed a internet nella segreteria utilizzato da marca modello

nr. 1 computer connesso in rete ed a internet nella segreteria utilizzato da marca modello

nr. 1 computer server connesso in rete ed a internet nella segreteria marca modello

nr. 1 computer connesso in rete ed a internet nello studio dell'avv. utilizzato dallo stesso marca modello

nr. 1 computer connesso in rete ed a internet nello studio dell'avv. utilizzato dallo stesso marca modello

nr. 1 computer connesso in rete ed a internet nella biblioteca utilizzato da 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 **Outlook Express**

Antivirus adoperato, sia sul server che su ogni singolo client.....

Firewall, adoperato sia sul server che su ogni singolo client.....

Titolare del trattamento è l'avv.....

Responsabile del trattamento è

Incaricati del trattamento sono:

Dr. (collaboratore di studio)

Dr. (collaboratore di studio)

..... (dipendente)

..... (dipendente)

Inoltre possono trattare i dati eventuali **sostituti di udienza** delegati ad hoc dal titolare, e **domiciliatari incaricati** dal titolare per le attività fuori del circondario del Tribunale di

Tecnico incaricato dell'assistenza e manutenzione degli strumenti elettronici è

I dati comuni dei clienti, dei fornitori o di terzi, i dati comuni di altri Avvocati e professionisti cui lo studio affida incarichi o si rivolge per consulenze, i dati giudiziari dei clienti, i dati giudiziari di terzi, i dati sensibili dei clienti e di terzi **sono trattati, oltre che dal titolare, anche da tutti gli incaricati.**

I dati **comuni del personale dipendente, i dati sensibili del personale dipendente, i dati afferenti i pagamenti a favore di terzi fornitori, la contabilità e i rapporti bancari dello studio sono tenuti dalla dipendente.....**, che si occupa della amministrazione. Questi dati non sono in rete, ma si trovano solo sul computer della segretaria; il trattamento di tali dati è fatto di regola dalla dipendente, ma anche gli altri incaricati sono autorizzati a conoscerli e trattarli.

Atteso che lo Studio tratta, oltre che dati comuni, anche **dati giudiziari e dati sensibili** (tra i quali anche eventuali dati genetici) di clienti o di terzi, per la custodia ed il trattamento di tali dati vengono adottate adeguate misure di protezione che ne contengano il rischio connesso alla gestione.

Per quanto riguarda gli strumenti elettronici, possono verificarsi malfunzionamenti, guasti, eventi naturali, alterazioni delle trasmissioni.

Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori, virus, intercettazioni dei dati.

Per quanto riguarda le aree ed i locali: possono essere colpiti da eventi naturali o accessi di terzi non autorizzati.

Va peraltro considerato nell'analisi concreta dei rischi il comportamento consapevole ed accorto degli incaricati (a cui sono state date specifiche istruzioni cui si attengono con diligenza), nonché l'aver adottato adeguate misure volte a scongiurare eventi pregiudizievoli relativi agli strumenti (accessi esclusivamente autorizzati, antivirus, firewall, contratto di assistenza software ed hardware), nonché l'aver adottato adeguate misure volte a prevenire eventi pregiudizievoli relative al contesto, quali accessi non consentiti ai locali, eventi accidentali (porta blindata, adeguamento alle norme della sicurezza).

Per ridurre i rischi sono state, infatti, adottate le seguenti misure:

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 stessa viene autonomamente scelta dall'**incaricato** e dallo stesso custodita in una busta chiusa che viene consegnata 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 inoltre crea apposita password per gli interventi del **tecnico** incaricato dell'assistenza.

Inoltre si è disposto che a tutti gli utilizzatori di strumenti elettronici non lascino incustodito, o accessibile, lo strumento elettronico stesso.

A tale riguardo, per evitare errori e dimenticanze, è stato inserito lo **screensaver** automatico dopo 5 minuti di non utilizzo, con ulteriore password per la prosecuzione del lavoro.

Si è inoltre disposto che si verifichi la provenienza delle email e non si operino operazioni di sharing.

Si è vietato la navigazione su siti di Hacking, cracking nonché di **scaricare software** da siti poco attendibili o non ufficiali; si è data disposizione di non aprire **messaggi di posta elettronica** e eseguire **files allegati** ai messaggi senza preventiva scansione antivirus. Nonché di non installare programmi scaricati da siti **non ufficiali** o comunque di natura incerta e di non dar credito a un messaggio pubblicitario dalle caratteristiche sospette. Si è data disposizione di tenere sempre attivata l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti sulla vostra macchina

Le email sono protette da antivirus e si è data disposizione che la casella di posta elettronica dello studio sia considerata strumento di lavoro ed utilizzata esclusivamente per esigenze lavorative, così come gli accessi ad internet vanno effettuati per dette finalità.

Essendo gli incaricati autorizzati a trattare la totalità dei dati, e comunque quelli sensibili e giudiziari, non si è provveduto a dare disposizioni in caso di **prolungata assenza** o impedimento dell'incaricato, eccezion fatta....

Ogni singolo computer è dotato di dispositivo antivirus di marca, e **firewall**.....che viene aggiornato con funzione automatica e con scansione per ogni aggiornamento antivirus, e comunque

settimanale.

Sul server è stato installato antiviruse 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 ed il firewall. E' stata data istruzione che, qualora nessun aggiornamento del sistema fosse segnalato automaticamente per un periodo di giorni 15, si provveda comunque ad attivare la funzione di controllo per verificare l'esistenza o meno di detti aggiornamenti automatici.

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, 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 il c.d. precedente.

Si è data disposizione che, **terminata la trattazione di una pratica**, ogni relativo file, o dato, esistente sui computer, sia cancellato.

Si è data disposizione di provvedere **periodicamente** alla pulizia dei file, all'eliminazione dei cookies, alla cancellazione della cronologia, alla deframmentazione, alla pulizia interna dell'hardware.

Si è data disposizione di farsi rilasciare dal tecnico installatore una descrizione scritta dell'intervento effettuato che ne **attesta la conformità** alle disposizioni del presente disciplinare tecnico.

Si è disposto che **non siano lasciati incustoditi** sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche in luoghi accessibili a terzi

non autorizzati. I fascicoli vanno conservati negli appositi schedari. In ogni caso, si è data disposizione che **il materiale cartaceo non deve essere visibile o visionabile dal cliente o da terzi** allorquando vengono autorizzati ad accedere allo studio del titolare o dei collaboratori ovvero alla postazione di lavoro degli incaricati.

Le **comunicazioni a mezzo posta**, o a mezzo telefax, dovranno essere tempestivamente smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento stampato dovrà essere prelevato e consegnato all'interessato.

Il **locale destinato all'archivio dovrà essere chiuso a chiave**. La dipendente è incaricata di controllare l'accesso all'archivio e tenere le chiavi. Fuori dall'orario di lavoro della dipendente l'accesso all'archivio è consentito previa autorizzazione del titolare.

Si è data istruzione che il **materiale cartaceo asportato** e destinato allo smaltimento dei rifiuti sia riposto negli appositi sacchi di plastica e che detti sacchi siano chiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detto materiale sia giornalmente asportato.

Analisi dei rischi:

Il **rischio di accesso ai locali** dello studio, può essere definito basso, atteso che l'ingresso allo studio è controllato, e che lo studio è dotato di citofono e chiusura con porta blindata.

Il **rischio di accesso ai singoli studi** può essere definito basso, atteso che gli stessi sono dotati di porte con chiusura e l'ingresso di terzi estranei avviene solo previa accettazione e controllo.

Il **rischio di accesso ai singoli strumenti** da parte di persone non autorizzate può essere definito basso, essendo controllato l'accesso allo studio da parte di terzi; la zona di attesa dei clienti distanziata dagli strumenti ed essendo gli stessi clienti controllabili dalla segreteria.

Le **aree ed i locali** potrebbero essere interessati da eventi naturali, quali incendi, allagamenti e corto circuiti, pur avendo lo studio provveduto ad adottare le disposizioni di sicurezza stabilite dalla L. 626/94. Essendo lo studio dotato di dispositivi salvavita, il rischio può comunque definirsi basso.

Per quanto riguarda gli **strumenti elettronici**, il rischio può essere definito basso, essendo state adottate dallo studio le misure di sicurezza, tendenti a ridurre il rischio gravante sui dati e derivante dalla gestione di detti strumenti.

Per quanto riguarda la **documentazione cartacea**, il rischio può essere definito basso, essendo l'archivio chiuso a chiave, le pratiche conservate negli schedari, ed essendo state adottate le altre misure indicate, fatta eccezione ovviamente per gli eventi naturali.

I telefax inviati su carta chimica sono stati riprodotti su carta normale per evitarne il deterioramento.

Per quanto riguarda i **supporti di memorizzazione**, il rischio di deterioramento dei dati da essi portati può essere ritenuto basso, attesi i frequenti back up, ed il fatto che essi sono conservati in un cassetto chiuso a chiave distante dal server , così come i dischi di installazione dei programmi software adottati.

Non vi sono **elaboratori non in rete**, per cui nessun giudizio di rischio deve essere dato su detti strumenti.

Atteso –infine- che gli **incaricati al trattamento** dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio afferente la riservatezza, o la distrazione, o l'incuria degli stessi, può essere definito basso.

Inoltre i dati, quanto comuni che sensibili, per gli affari trattati dallo Studio ed il tipo di clientela dello Studio non paiono essere, come detto, di particolare interesse per terzi.

Si ritiene che **verranno adottate** le seguenti ulteriori misure:

- sarà installato sistema di firma elettronica per la trasmissione delle e-mail.
- sarà inoltre adottata ogni altra misura che dal tecnico della manutenzione venisse ritenuta utile e necessaria per migliorare la sicurezza degli strumenti elettronici.
- sarà installato inoltre gruppo di continuità per il server.

Nell'ipotesi di **distruzione o danneggiamento dei dati o degli strumenti elettronici**, si è predisposto apposito piano di ripristino degli stessi, impartendosi comunque sin d'ora 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;
- reinstallati i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nel c.d. di back up;
- provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
- verrà dato incarico al tecnico manutentore di suggerire ogni altra misura;
- in ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;
- al fine di evitare eventi di perdita e di 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.

Incaricata di effettuare il salvataggio dei dati e di controllarne l'esito è la dipendente, ed in sua assenza alla dipendente.....

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. Destinatari della formazione sono i dipendenti e collaboratori. 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, per ogni dubbio, di richiedere al titolare.

La formazione è fatta dal titolare dello studio.

Pur essendo gli addetti già stati formati negli anni precedenti si è ritenuto opportuno tenere un **incontro di formazione**, anche sulle finalità e novità introdotte dalla nuova normativa.

Nel caso in cui il trattamento dei dati sensibili e/o giudiziari venga affidato a **soggetti esterni**, che li trattino con strumenti elettronici, per avere la garanzia che essi adottano le misure minime di sicurezza si esigerà dagli stessi una dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale attestino di aver adottato le misure minime 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.

Tutte le misure di sicurezza indicate, salvo quelle da attuarsi, devono intendersi in essere, e vengono sottoposte a verifica dal titolare nel corso dell'anno.

.....

Bozza predisposta dall' Avv. Antonio Rosa di Verona

Si consiglia di consultare il testo di M. Benasconi e L. Riva "Il nuovo codice

privacy: che fare?" (Diamint.com s.r.l.) e lo schema di DPS predisposto dal Garante, gli atti del Convegno 27.2.2004 di Verona (www.ilcaso.it)