Documento Programmatico Sicurezza per studio legale

Redatto ai sensi e per gli effetti dell'articolo 34. comma 1. lettera g) del D.Lgs. 196/2003 e del disciplinare tecnico (allegato B del D.Lgs. n. 196/2003)

SCOPO

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

In particolare nel Documento Programmatico Sulla Sicurezza vengono definiti i criteri tecnici e organizzativi per:

a. la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
b. i criteri e le procedure per assicurare l'integrità dei dati;
c. i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
d. l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

In conformità con quanto prescritto al punto 19 del Disciplinare tecnico (allegato B al D.Lgs.) nel presente documento si forniscono idonee informazioni riguardanti:

1) Elenco dei trattamenti di dati personali (punto 19.1) mediante:

1.1) individuazione dei dati personali trattati

1.2) descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti

1.3) l'elaborazione della mappa dei trattamenti effettuati

2) Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (punto 19.2)
3) Analisi dei rischi che incombono sui dati (punto 19.3)
4) Misure atte a garantire l'integrità e la disponibilità dei dati in essere e da adottare (punto 19.4)
5) Criteri e modalità di ripristino della disponibilità dei dati (punto 19.5)
6) Pianificazione degli interventi formativi previsti (punto 19.6)
7) Adozione misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno (punto 19.7)
8) Procedure per il controllo sullo stato della sicurezza
9) Dichiarazioni d'impegno e firma

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

1.1 Tipologie di dati trattati.

Il Documento Programmatico Sulla Sicurezza riguarda tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Lo Studio Legale tratta i seguenti dati:

dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali; dati comuni del personale dipendente, 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, 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 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.

I dati non pubblici vengono acquisiti previa l'informativa che si allega al presente D.P.S.

1.2 Aree, locali e strumenti con i quali si effettuano i trattamenti

Il trattamento dei dati avviene nella sede e luogo di lavoro, situata in ……., (es: zona centro, in palazzo d'epoca)

Gli uffici sono dislocati ……. (es: al primo *piano, l'accesso al piano è controllato da sistema di chiusura a scatto, l'accesso al locale ufficio* è *controllato attraverso suoneria d'ingresso)*

(Descrivere eventuali altre aree di trattamento ……..)

A. Schedari ed altri supporti cartacei

I supporti cartacei sono raccolti in schedari a loro volta custoditi come segue:

- Archivio 1 localizzato …….. ove in appositi armadi vengono archiviati i supporti cartacei di comune e continuo utilizzo;
- Archivio 2 localizzato ……. ove in appositi armadi e in locale al quale accedono solo le persone autorizzate vengono archiviati i supporti cartacei a fine ciclo lavorativo;
- ……
  ……

B. Elaboratori non in rete

Sono presenti n. ……. postazioni fisse non accessibili da altri elaboratori, situate…….

……

C - Elaboratori in rete

Si dispone di una rete, realizzata mediante collegamenti via cavo costituita da:

- n … server, localizzato nell'area ufficio
- n … postazioni lavoro dislocate nell'area ufficio
- n … stampanti di cui n … laser dislocate nell'area ufficio
- n … fax localizzato nell'area ufficio
- n … dispositivi di backup localizzati nell'area ufficio

Il sistema operativo del server è …..

Il sistema operativo dei computer è…

Lo studio adopera Internet Explorer versione …..

Lo studio adopera OutlooK Express …..

Lo studio per adopera per a gestione il sistema…

Antivirus adoperato …..

Firewall adoperato ….

D – Impianti di videosorveglianza

Sono/non sono utilizzati impianti di video-sorveglianza (eventualmente descriverli).

Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie di dati trattati emerge che:

1. solo i dati personali vengono trattati sistematicamente con supporti cartacei e con elaborazione;
2. i dati sensibili trattati con elaborazione, sono limitati a quelli necessari per assolvere agli obblighi normativi e contrattuali;
3. i dati giudiziari trattati sono quelli necessari per assolvere agli obblighi normativi e di Legge, essi comunque non vengono trattati con elaborazione;

4. gli elaboratori in rete pubblica presenti, non sono collegati in rete con altri, dispongono esclusivamente del collegamento a internet **(oppure altre ipotesi).**

1.3 Mappa dei trattamenti effettuati

Dal riepilogo dei dati trattati e dall'identificazione degli strumenti utilizzati si delinea il seguente schema:

Tipologia trattamento	Cartaceo	PC non in rete	PC in rete	Videosorveglianza
Dati comuni relativi a clienti				
Dati comuni relativi ad altri soggetti				
Dati biometrici relativi a clienti				
Dati idonei a rilevare la posizione di ..				
Dati di natura giudiziaria				
Dati relativi al personale				
Dati sensibili relativi a clienti				
Dati idonei a rilevare lo stato di salute				

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Titolare del trattamento dei dati

Per il trattamento dei dati personali il titolare…… non ha nominato responsabili, assumendo direttamente l'incarico di progettare, realizzare e mantenere in efficienza le misure di sicurezza.

oppure

Per il trattamento dei dati personali il titolare ha nominato il (i) seguente(i) responsabile(i)

(indicare i dati anagrafici e l'ambito di affidamento)

Soggetti incaricati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno

ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato, con il quale si individua l'ambito del trattamento consentito. Le lettere di incarico che vanno a completare il mansionario sono allegate al presente documento (allegato B).

Istruzioni specifiche fornite ai soggetti incaricati

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati sono fornite esplicite istruzioni relativamente a:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimuovibili contenenti dati personali;
- aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza;
- **(altro)**

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 esclusivamente tenuti dalla dipendente……., che si occupa della amministrazione. Questi dati non sono in rete ma si trovano solo sul computer della segretaria autorizzata a trattarli **o altro**.

3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

L'analisi dei possibili rischi che gravano sui dati è stata effettuata tenendo conto di due tipi di rilevazioni:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- le caratteristiche degli strumenti utilizzati per il trattamento dei dati.

Riguardo il primo aspetto l'analisi dei rischi si può così sintetizzare:

per i dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali), i 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 disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi), i dati comuni di terzi (forniti dai clienti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari) i dati comuni dei fornitori (concernenti la reperibilità e la corrispondenza con gli

stessi, nonché inerenti ai rapporti fiscali) i dati comuni di altri avvocati e professionisti cui lo studio affida incarichi (quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) ed i dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali: il rischio legato alla loro gestione può definirsi basso/medio.

Per i dati sensibili del personale dipendente, i dati giudiziari dei clienti, i dati giudiziari di terzi, i dati sensibili dei clienti (dagli stessi forniti per l'espletamento degli incarichi affidati allo studio) i dati sensibili di terzi (forniti dai clienti per l'espletamento degli incarichi affidati allo studio) il rischio legato alla loro gestione è da definirsi medio, eccezion fatta per i dati riguardanti le pratiche in cui sono contenuti 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 questi ultimi dati il rischio collegato alla gestione può definirsi alto.

Per i dati sensibili afferenti cause di stato (esempio disconoscimento di paternità) il rischio di gestione può essere definito maggiormente elevato.

Riguardo gli strumenti impiegati nel trattamento sono stati individuati come sorgenti soggette a rischio le seguenti categorie di strumenti utilizzati per il trattamento:

Strumenti	Legenda
Schedari e altri supporti cartacei custoditi nell’area controllata	A
Elaboratori non in rete custoditi nell’area controllata	B
Elaboratori in rete custoditi nell’area controllata	C

Fattori di rischio	Basso	Medio	Elevato
Rischio legato ad accesso non autorizzato nei locali, asportazione e furto di strumenti contenenti dati			A B C
Rischio guasti tecnici hardware, software, supporti		C	B
Rischio penetrazione reti di comunicazione, azione di virus informatici, spamming o altre tecniche di sabotaggio		B	C
Rischio legato ad errori umani, comportamenti sleali o fraudolenti, disattenzione o incuria	A	B	C
Rischio per possibili eventi distruttivi			A B C

4. MISURE ATTE A GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI IN ESSERE E DA ADOTTARE.

Alla luce dei fattori di rischio e delle aree individuate nel precedente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito degli strumenti elettronici

Le successive misure indicate a sostegno della fase di protezione dei dati si suddividono in:

- misure già adottate al momento della stesura del presente documento;
- ulteriori misure finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati.

4.1 La protezione di aree e locali

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, i locali ove si svolge il trattamento dei dati sono protetti da:

- dispositivi antincendio previsti dalla normativa vigente
- gruppo di continuità dell'alimentazione elettrica
- impianto di condizionamento
- altro ……

Sono adottate le seguenti misure per impedire accessi non autorizzati (elencare):

Il locale destinato all'archivio dovrà essere chiuso a chiave. La dipendente

…….. è incaricata di controllare l'accesso all'archivio. Fuori dall'orario di lavoro l'accesso all'archivio è consentito previa registrazione.

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.

……

……

4.2 Custodia e archiviazione dei dati

Agli incaricati sono state impartite istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti. In particolare sono state fornite direttive per:

- il corretto accesso ai dati personali, sensibili e giudiziari;
- la conservazione e la custodia di documenti, atti e supporti contenenti dati personali, sensibili e giuridici;
- la definizione delle persone autorizzate ad accedere ai locali archivio e le modalità di accesso;
- non lasciare incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche. I fascicoli vanno conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti;
- assicurare che le comunicazioni a mezzo posta, o a mezzo telefax, siano tempestivamente smistate e consegnate ai destinatari;
- (altro)

4.3 Misure logiche di sicurezza

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici; in particolare ciascun incaricato deve essere dotato 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. Le password dovranno essere automaticamente disattivate dopo tre mesi di non utilizzo;
- autorizzazione e definizione delle tipologie di dati ai quali gli incaricati posso accedere e utilizzare al fine delle proprie mansioni lavorative;
- protezione di strumenti e dati da malfunzionamenti e attacchi informatici;
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali;
- (altro)

Accesso ai dati e istruzioni impartite agli incaricati

Gli incaricati al trattamento dei dati, dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici

(username e password);

- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo di assoluta riservatezza;
- divieto di divulgazione della password di accesso al sistema;
- altro …….

Protezione di strumenti e dati

Premesso che non vengono (oppure che vengono) trattati dati sensibili e giudiziari in rete, il sistema di elaborazione è comunque protetto da programmi antivirus e di sistema firewall anti-intrusione. Il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione.

Agli incaricati è stato affidato il compito di aggiornare periodicamente (precisare la periodicità) il sistema di protezione.

Supporti rimovibili

Anche se le norme prevedono particolari cautele solo per i supporti rimovibili contenenti dati sensibili e giuridici, la tutela per il trattamento viene estesa ai dati personali come segue:

- custodia dei supporti in contenitori chiusi a chiave in locali con accesso ai soli autorizzati;
- cancellazione e/o distruzione del supporto una volta cessate le ragioni per la conservazione;
- altro ……

5. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema. Il salvataggio dei dati avviene:

- con frequenza giornaliera/settimanale/mensile
- le copie vengono custodite in un luogo protetto

Custode di detti backup è stato nominato l'incaricato ……. Si è data disposizione che, effettuato un backup, venga distrutto il c.d. precedente.

6. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Agli incaricati al trattamento, il titolare (direttamente o tramite soggetti da lui identificati) fornisce la necessaria formazione:

- al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansione
- in occasione dell'introduzioni di nuovi strumenti e programmi informatici

La formazione ad ogni modo deve avere una frequenza annuale (o……). 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.

7. TRATTAMENTI AFFIDATI ALL'ESTERNO

Nello svolgimento dell'attività, vengono/non vengono affidati dati personali all'esterno *(nel caso il trattamento venga affidato all'esterno sono state*

impartite istruzioni per iscritto al terzo destinatario, al fine di rispettare quanto prescritto dal codice della privacy).

Il soggetto cui le attività sono affidate dichiara:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

8. CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA

Il titolare (il responsabile per la sicurezza) mantiene aggiornate le misure di sicurezza al fine di adottare gli strumenti più idonei per la tutela dei dati trattati. Egli verifica inoltre con frequenza almeno mensile l'efficacia delle misure adottate relativamente a:

- accesso fisico a locali dove si svolge il trattamento
- procedure di archiviazione e custodia dati trattati
- efficacia e utilizzo misure di sicurezza strumenti elettronici
- integrità dei dati e delle loro copie di backup
- distruzione dei supporti magnetici non più riutilizzabili

- livello di informazione degli interessati

9. DICHIARAZIONE D'IMPEGNO E FIRMA

Il presente documento redatto in data ……. viene firmato in calce da……. In qualità di titolare, e verrà aggiornato periodicamente entro il 31 marzo di ogni anno.

L’originale del presente documento è custodito presso la sede della società, per essere esibito in caso di controllo.

Una copia verrà consegnata ai responsabili di determinati trattamenti di dati appositamente nominati.

Data e luogo

Firma del Titolare

_____

Allegato A

Organigramma privacy

TITOLARE DEI DATI

RESPONSABILI	INCARICATI AL TRATTAMENTO
……..	……..
……..	……..
……..	……..
……..	……..