progetto MAAT Universita' degli Studi di Milano	Document name: MODELLO PER STUDI LEGALI – DOCUMENTO PROGRAMMATICO DELLA SICUREZZA ai sensi dell'art. 34 lett. g) D. Lgs. 196/2003 e regola 19 allegato B al D. Lgs. 196/2003 Autore: Dott. Filippo Pappalardo	Global Document Number: 1
Version: 3.0	Date:31/03/2004	
Revisioni successive di	Date	
Dott. Filippo Pappalardo	20/05/2004	

In collaborazione con

ORDINE DEGLI AVVOCATI DI MILANO

UNIVERSITA' DEGLI STUDI DI MILANO
ISTITUTO DI FILOSOFIA
E SOCIOLOGIA DEL DIRITTO
VIA FESTA DEL PERDONO, 7 - 20122 MILANO

MODELLO PER STUDI LEGALI DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

ai sensi dell'art. 34 lett. g) D. Lgs. 196/2003 e regola 19 allegato B al D. Lgs. 196/2003

Dott. Filippo Pappalardo : pappalardo@fildir.unimi.it

Le note di commento al testo sono riportate in rosso e in formato ridotto

In allegato le tabelle pronte all'uso, l'informativa e la lettera d'incarico

Il documento è aggiornato con le ultime considerazioni dell'Autorità Garante della privacy

Il documento è suddiviso in tre parti:

- **Modello di D.P.S. con note (da pag. 3 a pag. 16)**
- **Modello di D.P.S. organizzato in tabelle pronte all'uso (da pag. 17 a pag. 32)**
- **Allegati (informativa pag. 33 e lettera d'incarico pag. 34)**

INDICE

PARTE I

PARTE II

ALLEGATI

0. INTRODUZIONE

Scopo di questo documento è delineare il quadro di sicurezza del **sistema informativo** dello

Studio Legale _____

Seguono i dati identificativi dello Studio Legale:

Es: Via Verdi 1, 20100 MILANO

DEFINIZIONI

Per **sistema informativo** s'intende l'insieme delle risorse umane, delle regole organizzative, delle risorse hardware e software (applicazioni e dati), dei locali e della documentazione che, nel loro complesso, consentono di acquisire, memorizzare, elaborare, scambiare e trasmettere informazioni inerenti alle attività dello studio legale.

I dati personali contenuti nel sistema informativo **devono essere protetti** adottando le misure minime di sicurezza previste dal D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali" (d'ora in poi codice) artt. 33-36, con le modalità descritte dal **disciplinare tecnico allegato B** al codice stesso.

Ai fini del **D. Lgs. 196/2003** si intende per:

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 di dati;

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'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 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 61 del codice di procedura penale;

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 dal responsabile;

i) "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

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;

n) "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) "**banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) "**Garante**", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

[…]

Ai fini del **D. Lgs. 196/2003** si intende, inoltre, per:

a) "**misure minime**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

b) "**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

e) "**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g) "**sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

IL TITOLARE DEI DATI

Studio Legale / Avv. _____ (* obbligatorio)

Titolare (2): Studio Legale / Avv. _____ (* facoltativo)

Il titolare dello Studio Legale svolge le funzioni di "**titolare del trattamento dei dati personali**" e decide riguardo alle modalità di trattamento e agli strumenti utilizzati, ivi **compreso il profilo della sicurezza**. Il titolare può essere una **persona fisica** (ad esempio: avvocato singolo), una **persona giuridica** (ad esempio: società tra avvocati) […], **associazione** (ad esempio: associazione tra professionisti) od organismo (art. 4 lett. f) del codice). E' previsto, inoltre, che le decisioni possano essere prese **anche unitamente ad altro titolare** (art. 4 lett. f) del codice).

Il Titolare del trattamento dei dati:

- adotta (art. 31 "codice"), riguardo al trattamento di dati personali, le **misure minime di sicurezza** (art. 33 "codice") con le modalità previste dal Titolo V, Capo II del "codice" e dal disciplinare tecnico contenuto nell'allegato B) del "codice" stesso;
- adotta il **documento programmatico della sicurezza entro il 31 marzo di ogni anno**, ai sensi della regola 19 all. B del codice, vigilando sulla sua effettiva applicazione.
  Per il 2004 il termine è stato prorogato al 30 giugno (parere Garante Privacy 22 marzo 2004).
- nel caso in cui per obiettive ragioni tecniche, all'entrata in vigore del codice, non fosse stato possibile applicare immediatamente, in tutto o in parte, le misure minime di sicurezza (ivi compreso il piano di sicurezza), il titolare avrà provveduto alla **redazione di un documento a data certa descrivente tali ragioni, da conservare presso la propria struttura**. (art. 180 c.2 del codice).
  In casi come questo l'adeguamento degli strumenti elettronici è previsto entro e non oltre il 1° gennaio 2005. (art. 180 c.3 del codice).

In casi particolari il Titolare:

- adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, ricevendo dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico allegato al "codice" (art. 25 all. B "codice");

- verifica l'adeguamento delle misure minime di sicurezza previste per la protezione dei dati personali all'aggiornamento periodico predisposto dal Ministro della Giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore (art. 36 del "codice").

Il Responsabile designato ai sensi dell'art. 4 lett. g) del codice è:

Avv. / Dott. / Sig. _____ (* facoltativo)

Si tratta della persona (fisica o giuridica) preposta dal Titolare al trattamento dei dati personali.

Per la stesura del Documento Programmatico della Sicurezza è necessario dare corso alle seguenti operazioni:

- Fornire l'elenco dei trattamenti di dati personali effettuati dalla struttura (19.1 all. B codice);
- Distribuire i compiti e le responsabilità nell'ambito delle strutture preposte al trattamento dei dati. Elencare le informazioni anagrafiche ed organizzative relative al personale, specificando a quali aree, riguardo il trattamento di dati personali, può accedere, e quali apparecchiature può utilizzare (19.2 all. B codice);
- Analizzare i rischi che incombono sui dati (19.3 all. B codice);
- Descrivere i 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 (19.7 all. B codice);
- Studiare un piano per la protezione fisica delle aree e dei locali, rilevanti ai fini della custodia e accessibilità dei dati (19.4 all. B codice);
- Descrivere i criteri e le modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni (19.5 e 23 all. B codice);
- Adottare le misure necessarie a garantire l'integrità e la disponibilità dei dati (19.4 all. B codice);
- Prevedere 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 formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali (19.6 all. B codice);

ADOTTA IL SEGUENTE

DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

1. ELENCO DEI TRATTAMENTI DI DATI DELLO STUDIO LEGALE

- dati personali dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali; (cod. 01)

- dati personali 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; (cod. 02)

- dati personali 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; (cod. 03)

- dati personali 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; (cod. 04)

- dati personali dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria; (cod. 05)

- dati personali 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; (cod. 06)

- 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; (cod. 07)

- dati giudiziari dei clienti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR n. 313/2002, o idonei a rivelare al qualità di imputato o indagato; (cod. 08)

- dati giudiziari di terzi, idonei a rivelare i provvedimenti di cui all'art. 3 DPR n. 313/2002, o idonei a rivelare al qualità di imputato o indagato; (cod. 09)

- 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; (cod. 10)

- dati sensibili dei clienti, dagli stessi forniti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute; (cod. 11)

- dati sensibili di terzi, forniti dai clienti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute; (cod. 12)

- dati sensibili di clienti o terzi, comunque afferenti la vita sessuale. (cod. 13)

Per ogni trattamento elencare e descrivere i dispositivi di accesso e le caratteristiche d'interconnessione.

2. RUOLI, COMPITI E RESPONSABILITA'

SEZIONE LEGALE: AVVOCATO / I e PATROCINATORE / I

Comprende le operazioni di trattamento necessarie allo svolgimento di attività:

- giudiziale
- stragiudiziale
- consulenza legale
- _____

Elenco trattamenti: _____ Riportare i codici indicati nella sezione 1

SEZIONE PRATICANTATO: PRATICANTE / I

Comprende le operazioni di trattamento necessarie allo svolgimento di attività:

- archivio / ufficio
- assistenza alle udienze
- _____

Elenco trattamenti: _____ Riportare i codici indicati nella sezione 1

SEZIONE SEGRETERIA:

Comprende le operazioni di trattamento necessarie allo svolgimento di attività:

- archivio / ufficio
- amministrazione / rapporti di lavoro
- _____

Elenco trattamenti: _____ Riportare i codici indicati nella sezione 1

L'accesso ai dati personali e al loro trattamento con strumenti informatici da parte dei soggetti facenti parte delle varie SEZIONI dello Studio, è regolato in base alle seguenti misure minime di sicurezza:

i) **Sistema di autorizzazione**. Devono essere specificati l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del **Profilo di autorizzazione** del richiedente (c.d. "sistema di autorizzazione" ex art. 4 g) del codice e artt. 12-14 allegato B del codice).

ii) **Credenziali di autenticazione**. Si tratta di strumenti che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti (art. 1 all. B "codice").
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato ("user ID") che non può essere assegnato ad altri incaricati, neppure in tempi diversi (art. 6 all. B "codice"), associato a una parola chiave riservata conosciuta solamente dal medesimo incaricato (art. 2 all. B "codice");

N.B.: Questa parte può essere inserita nel DPS, richiamata dal DPS come allegato o prevista come documento separato.

i) SISTEMA DI AUTORIZZAZIONE

Il sistema di autorizzazione informatica utilizzato è: _____

Ad esempio: Rete informatica con sistema operativo multiutenza (Win2000/NT, MacOS X, Linux). Oppure accesso consentito tramite lettore smart card / firma digitale o ancora chiavi biometriche. In ogni caso, qualsiasi soluzione in grado di permettere accessi differenziati ai dati.

Per il trattamento senza l'ausilio di strumenti elettronici: regole 28, 29 e 30 dell'allegato B al codice.

PROFILI DI AUTORIZZAZIONE

(Utilizzare specifiche lettere d'incarico per impartire istruzioni scritte agli incaricati – vedi all. 2)

AVVOCATI e PRATICANTI

Il/La Avv./Dott. _____

in qualità di avvocato/praticante presso lo Studio Legale _____ Qualifica: TIT., RESP., INC. è autorizzato al trattamento dei dati personali relativi a: (riprendere da elenco trattamenti – E' possibile identificarli con un codice) e ad accedere alle seguenti aree:

Es: Aree di accesso: **BANCA DATI**: Ad es: NOMEFILE.DATABASE / DISCO RIGIDO SU PC/MAC (MARCA, MODELLO, UBICAZIONE, IN CONDIVISIONE) / **ARCHIVIO CARTACEO**: (UBICAZIONE, POSSESSO CHIAVI) / …

FINO AL 30/6/2005

(Il 31/3/2005 l'autorizzazione verrà rinnovata fino all'anno successivo)
(almeno 1 volta l'anno le autorizzazioni vanno rinnovate)

(ripetere per ogni avvocato e/o praticante dello Studio)

DIPENDENTI

Il/La Sig./Sig.ra/Dott. _____

in qualità di dipendente presso lo Studio Legale _____ Qualifica: TIT., RESP., INC. è autorizzato al trattamento dei dati personali relativi a: (riprendere da elenco trattamenti – E' possibile identificarli con un codice) e ad accedere alle seguenti aree:

Es: Aree di accesso: **BANCA DATI**: Ad es: NOMEFILE.DATABASE / DISCO RIGIDO SU PC/MAC (MARCA, MODELLO, UBICAZIONE, IN CONDIVISIONE) / **ARCHIVIO CARTACEO**: (UBICAZIONE, POSSESSO CHIAVI) / …

FINO AL 30/6/2005

(Il 31/3/2005 l'autorizzazione verrà rinnovata fino all'anno successivo)
(almeno 1 volta l'anno le autorizzazioni vanno rinnovate)

(ripetere per ogni dipendente dello Studio)

---

ii) CREDENZIALI DI AUTENTICAZIONE

ASSEGNAZIONE CREDENZIALI DI AUTENTICAZIONE – AVVOCATI

Avv. _____ / anagrafica dell'avv.

Trattamento consentito ad esempio: **dati personali, sensibili, giudiziari o comunque riprendere da elenco trattamenti**

UserID: _____ | *Password: ******** (almeno 8 caratteri e non facilmente riconducibile all'incaricato)* |

Aree di accesso: IN BASE AL TRATTAMENTO PER IL QUALE E' AUTORIZZATO

Data di attivazione: 30/6/2004 | Data di rinnovo: **30/12/2004 // 30/9/2004** (6 mesi / almeno ogni 3 mesi se il trattamento riguarda dati sensibili e giudiziari)

ASSEGNAZIONE CREDENZIALI DI AUTENTICAZIONE – PRATICANTI

Dott. _____/anagrafica praticante

Trattamento consentito ad esempio: **dati personali e giudiziari o comunque riprendere da elenco trattamenti**

UserID: _____ | *Password: ******** (almeno 8 caratteri e non facilmente riconducibile all'incaricato)* |

Aree di accesso: IN BASE AL TRATTAMENTO PER IL QUALE E' AUTORIZZATO

Data di attivazione: 30/6/2004 | Data di rinnovo: **30/12/2004 // 30/9/2004** (6 mesi / almeno ogni 3 mesi se il trattamento riguarda dati sensibili e giudiziari)

ASSEGNAZIONE CREDENZIALI DI AUTENTICAZIONE – DIPENDENTI

Sig./Sig.ra. _____/anagrafica dipendente

Trattamento consentito: **dati personali**

UserID: _____ | *Password: ******** (almeno 8 caratteri e non facilmente riconducibile all'incaricato)* |

Aree di accesso: IN BASE AL TRATTAMENTO PER IL QUALE E' AUTORIZZATO

Data di attivazione: 30/6/2004 | Data di rinnovo: **30/12/2004** (almeno ogni 6 mesi se il trattamento riguarda dati personali)

ASSEGNAZIONE CREDENZIALI DI AUTENTICAZIONE – TECNICI

Sig./Sig.ra./Dott. _____ (area tecnica) | Trattamento consentito: -

Aree di accesso: solo gestione tecnica

UserID: _____ | Password: ******

Data di attivazione: 30/6/2004 – Data di rinnovo: --

Note: Le password non vanno riportate nel D.P.S. o in qualsiasi altro documento.

Esse sono segrete ed i soggetti incaricati della loro custodia vengono preventivamente incaricati per iscritto a svolgere tale compito (art. 10 allegato B codice).

CREDENZIALI DI AUTENTICAZIONE - GARANZIE

Il Titolare garantisce la segretezza delle copie delle credenziali di autenticazione e indica

Il/La Avv./Sig./Sig.ra./Dott. _____ come incaricato della custodia della componente riservata delle credenziali di autenticazione, il/la quale informa tempestivamente gli incaricati di un eventuale intervento operato per necessità di operatività e sicurezza del sistema.

Le credenziali di autenticazione non utilizzate da almeno **sei** mesi (**tre** mesi per dati sensibili e giudiziari) sono **disattivate**, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (art. 7 all. B “codice”).

Le credenziali sono **disattivate** anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali (art. 8 all. B “codice”).

Ad ogni incaricato possono essere assegnate o associate individualmente **una o più credenziali** per l'autenticazione (art. 3 all. B “codice”).

3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

- Rivelazione (comunicazione o diffusione) illegittima di informazioni da parte di soggetti interni o terzi;

Ad esempio, sarebbe opportuno disporre che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche. Solitamente, i fascicoli vanno conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti. Analogamente, per quanto riguarda gli strumenti informatici, sarebbe opportuno spegnere il computer se ci si assenta per un periodo di tempo lungo. Un computer acceso è, in linea di principio, maggiormente vulnerabile sia in loco che tramite accesso remoto. Anche per questi motivi non è consentito lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro. (art. 9 all. B "codice"). Un'ottima idea potrebbe essere un salvaschermo con password. Inoltre, è buona norma prevedere un sistema sicuro di smaltimento dei rifiuti cartacei (i c.d. tritacarte) ed utilizzare software appositi per la rimozione sicura di files dai supporti informatici.

- Distruzione o perdita dei dati stessi (anche accidentale);

Ad esempio: Per i sistemi informatici installare un gruppo di continuità per l'alimentazione continua. Infatti, i black-out improvvisi sono tra le maggiori cause di danni o perdita di dati da parte degli strumenti elettronici.

- Accesso non autorizzato ai dati, da parte di soggetti interni non autorizzati ad un determinato trattamento o da parte di terzi;

Ad esempio, è necessario utilizzare un sistema di autenticazione informatica in grado di permettere l'accesso al trattamento dei dati ai soggetti autorizzati a quel (e solo a quello) determinato trattamento. A livello di sistema operativo non per tutti è possibile effettuare questa operazione. Sistemi operativi in grado di svolgere questa funzione sono, tra gli altri, Windows 2000, Mac OS X, Linux.

- Trattamento non consentito di dati da parte di soggetti non abilitati;

Ad esempio, affidare a terzi un trattamento di dati senza nessuna autorizzazione. Consentire l'accesso agli strumenti informatici e agli archivi dello Studio a persone non autorizzate o non abilitate.

- Trattamento eccedente le finalità per le quali i dati sono stati raccolti.

Ad esempio, far riferimento ai dati dei propri clienti, acquisiti in ragione della professione svolta, per altre attività.

Per ogni punto è necessario mettere in relazione le misure di sicurezza con gli eventi potenzialmente dannosi per la sicurezza dei dati, le possibili conseguenze e la loro gravità. Il riferimento è la regola 19.3 allegato B al Codice.

4. MISURE ADOTTATE PER GARANTIRE INTEGRITA' E DISPONIBILITA' DEI DATI

Queste misure riguardano tutti i tipi di trattamento dati descritti nella sezione 1.

1) PROTEZIONE FISICA DELLE AREE E DEI LOCALI
AI SENSI DELLA REGOLA 19.4 ALLEGATO B DEL CODICE

a) Sistema di protezione anti-intrusione / antincendio: ES. PORTA BLINDATA / TAGLIAFUOCO;

b) Sicurezza archivio cartaceo: ES. PROTEZIONE CON SERRATURA DEDICATA;

c) Eventuali aree facilmente accessibili: ES. SALA DI ASPETTO / SEGRETERIA (descrizione accessi)

d) Eventuali impianti di controllo accessi: ES. TESSERA DI RICONOSCIMENTO / REGISTRO entrate/uscite

Responsabile controllo periodico efficienza: _____ Misure a) b) c) d)

2) PROTEZIONE INFORMATICA DEGLI STRUMENTI ELETTRONICI
AI SENSI DELLA REGOLA 19.4 ALLEGATO B DEL CODICE

e) Sistema operativo in uso: QUELLI CHE GARANTISCONO EFFETTIVAMENTE DI ATTIVARE CREDENZIALI DI AUTENTICAZIONE (es. Windows 2000, Mac OS X, Linux …)

f) Installazione software in grado di prevenire vulnerabilità e/o correggere difetti degli strumenti elettronici: ES. PATCH DI WINDOWS (almeno ogni 6 mesi, 3 mesi se il trattamento riguarda dati sensibili o giudiziari)

Nota: Per patch, letteralmente "pezza", s'intende qualsiasi istruzione o codice rilasciata dal produttore di un determinato software per ovviare a inconvenienti relativi al funzionamento o alla sicurezza dello stesso.

g) Software antivirus installato: _____ data ultimo aggiornamento: _____ (aggiornamento successivo massimo 6 mesi)

Nota: In realtà sarebbe opportuno un aggiornamento molto più frequente, quasi giornaliero.

h) Software firewall installato: _____ data ultimo aggiornamento: _____

Nota: Un firewall, letteralmente "muro di fuoco" è un software che permette di monitorare ed inibire gli accessi da remoto alla propria rete informatica. E' una misura minima di sicurezza prevista per il trattamento di dati sensibili e/o giudiziari (art. 20 allegato B al codice).

Responsabile controllo periodico efficienza: _____ Misure e) f) g) h)

Le misure descritte alle lettere _____ sono già in essere.

Le misure descritte alle lettere _____ sono da adottare.

Per ogni punto è necessario compilare una scheda come quelle sopra descritte, con la quale indicare se la misura è già operativa, o da che data è operativa, e verificarne periodicamente l'efficienza.

5. RIPRISTINO DISPONIBILITA' DEI DATI DISTRUTTI O DANNEGGIATI

Il salvataggio dei dati (distinguere dati personali, sensibili e giudiziari ed indicare banche dati se esistenti) (c.d. back-up) viene effettuato con **frequenza settimanale** (regola 18 allegato B codice) attraverso la seguente procedura: _____ ES: utilizzo unità di back-up MARCA, MODELLO (MASTERIZZATORE, HARD DISK ESTERNO, …)

Le copie vengono conservate con le seguenti modalità: _____

Incaricato salvataggio dati:

Avv./Dott./Sig./Sig.ra _____

I supporti rimovibili utilizzati per il back-up vengono conservati con le seguenti modalità:

ES.: ARMADIO A MURO CON SERRATURA (UBICAZIONE)

Incaricato custodia supporti di back-up:

Avv./Dott./Sig./Sig.ra _____

La verifica della leggibilità del supporto viene effettuata: ES.: IL 28 DI OGNI MESE (TEST SALVATAGGIO / RIPRISTINO)

In caso di necessità, il ripristino avviene attraverso la seguente procedura: Ad esempio, copia files da supporto di backup … della banca dati / files _____

Note: Il ripristino dei dati o degli strumenti elettronici in caso di distruzione o danneggiamento (19.5 allegato B codice) è previsto (almeno) entro 7 giorni dall'evento dannoso (art. 23 allegato B codice).

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (art. 22 All. B "codice");

appena terminate le operazioni, i supporti di back-up su cui sono memorizzati i dati vengono custoditi al fine di evitare accessi non autorizzati e trattamenti non consentiti (art. 21 All. B "codice").

6. DESCRIZIONE DELLE ATTIVITA' DI FORMAZIONE

Gli argomenti oggetto di formazione per gli incaricati del trattamento dei dati riguardano (19.6 allegato B del codice):

- Conoscenza dei rischi che incombono sui dati;
- Misure disponibili di attività fisiche, logiche e informatiche per prevenire eventi dannosi;
- Disciplina sulla protezione dei dati personali in rapporto alle relative attività;
- Profili di responsabilità in merito al trattamento dei dati.

Interventi formativi programmati:

Data: _____ Argomento (descrizione): _____ Relatore: _____

Data: _____ Argomento (descrizione): _____ Relatore: _____

e i relativi calendari.

N.B.: Indicare i soggetti interessati dai corsi di formazione (specificare se vi sono soggetti già formati o da formare durante l'anno su determinati argomenti).

Note:

Nel corso dell'anno sono previste altre attività di formazione nel caso in cui vi siano cambiamenti di mansioni, o introduzione di nuovi significativi strumenti rilevanti ai fini del trattamento dei dati personali.

7. DATI PERSONALI AFFIDATI, IN CONFORMITA' AL CODICE, ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE

Nota:

Il titolare del trattamento dei dati deve stabilire i criteri da adottare per garantire l'adozione delle misure minime di sicurezza nel caso in caso il trattamento dei dati personali venga affidato all'esterno della struttura (19.7 allegato B codice).

Ad esempio, sarebbe opportuno prevedere che il trasporto di fascicoli o files dallo studio legale al domicilio di un avvocato / praticante / dipendente fosse subordinato all'adozione da parte di questi soggetti di particolari misure di sicurezza fisiche e telematiche (custodia accurata del fascicolo cartaceo, cifratura dei dati elettronici).

Per quanto riguarda, invece, l'affidamento presso soggetti terzi, il titolare è tenuto a descrivere l'attività che è stata delegata e quali tipi di dati in essa vengono trattati.

Per ogni operazione o gruppo di operazioni su dati personali, effettuati all'esterno della struttura, sarebbe consigliabile creare una modulistica di questo tipo:

Il trattamento di dati personali (indicare se sensibili e giudiziari) relativo a _____ (specificare) viene affidato a: (persona fisica / persona giuridica) _____ (< inserire i dati relativi)

in data _____ fino a _____ (data / tempo indeterminato).

Il soggetto indicato ha rilasciato dichiarazione di conformità alle misure minime di sicurezza della sua struttura. Tale dichiarazione fa parte di un impegno assunto su base contrattuale. Il documento è conservato presso questo Studio Legale.

***

(ATTENZIONE: nella modulistica allegata il documento sottostante non viene riportato perché non va inserito nel d.p.s.)

Il/La sottoscritto/a (società), al/alla quale è stato affidato il trattamento è consapevole che i dati personali sono soggetti all'applicazione del codice. Egli/Essa dichiara di aver adottato le misure minime di sicurezza previste dagli artt. 33 – 36 del D. Lgs. 196/2003, e di effettuare il trattamento dei dati con le seguenti modalità: _____ (con/senza strumenti elettronici)

Il/La sottoscritto/a (società) relaziona annualmente lo studio legale sulle misure di sicurezza adottate. Il titolare dello Studio ha il diritto di verificare periodicamente l'effettiva adozione delle misure di sicurezza presso la nostra struttura.
Il/La sottoscritto/a (società) è autorizzato/a al trattamento dei dati relativi a _____ (definire quale/i trattamenti) in nome e per conto del titolare _____dello studio legale _____ (riportare tutti i dati).

Firma _____

8. TUTELA DEI DATI PERSONALI IDONEI A RIVELARE LO STATO DI SALUTE O LA VITA SESSUALE (*)

I dati personali idonei a rivelare lo stato di salute o la vita sessuale (cfr. 24 allegato B del codice) sono cifrati o separati dagli altri dati personali dell'interessato (19.8 allegato B codice).

(*) La regola 24 chiama in causa direttamente gli organismi sanitari e gli esercenti le professioni sanitarie ma sembra difficile immaginare un diverso trattamento di questi dati presso altri tipi di struttura. Ad esempio, la custodia di una perizia medica di una delle parti in causa presso lo studio legale giustifica l'adozione della misura di sicurezza qui descritta.

I dati personali idonei a rivelare lo stato di salute o la vita sessuale vengono cifrati attraverso il software (o con le seguenti modalità): _____ (Ad esempio: PGP oppure l'apposita funzione di molti software di firma digitale)

e sono contenuti in: cartella / computer / banca dati separata.

Questa è la formula che si adatta meglio al trattamento di dati con l'ausilio di strumenti elettronici.

I dati personali idonei a rivelare lo stato di salute o la vita sessuale vengono conservati in un apposito archivio separato situato in: _____ L'archivio è dotato di BLINDATURA / SERRATURA SPECIALE / ALTRO…

Questa, invece, è la formula che si adatta meglio al trattamento di dati senza l'ausilio di strumenti elettronici.

Il presente documento programmatico della sicurezza è stato redatto, ai sensi dell'art. 34 del D. Lgs. 196/2003 e della regola 19 allegato B al codice da:

(QUALIFICA, NOME, COGNOME, TITOLARE/RESPONSABILE) _____

in data _____ (termine ultimo attuale: 30 giugno 2004)

E' composto di n. pag. _____

Rimane a disposizione degli organi competenti presso la struttura che lo ha redatto.

Note: NON VA INVIATO AL GARANTE PRIVACY

E' valido a tutti gli effetti di legge fino a: **31 marzo ….**

Milano, lì _____ Firma _____

In collaborazione con

ORDINE DEGLI AVVOCATI DI MILANO

UNIVERSITA' DEGLI STUDI DI MILANO
ISTITUTO DI FILOSOFIA
E SOCIOLOGIA DEL DIRITTO
VIA FESTA DEL PERDONO, 7 - 20122 MILANO

MODELLO PER STUDI LEGALI
DOCUMENTO PROGRAMMATICO
DELLA SICUREZZA

ai sensi dell'art. 34 lett. g) D. Lgs. 196/2003
e regola 19 allegato B al D. Lgs. 196/2003

Dott. Filippo Pappalardo : pappalardo@fildir.unimi.it

Le tabelle pronte all'uso

Il testo è modificabile in ogni sua parte ed è fornito a titolo esemplificativo

Scopo di questo documento è delineare il quadro di sicurezza del **sistema informativo** dello

Studio Legale _____

Via _____, 20_____ MILANO

IL TITOLARE DEI DATI

Studio Legale / Avv. _____ (* obbligatorio)

Titolare (2): Studio Legale / Avv. _____ (* facoltativo)

Il Responsabile designato ai sensi dell'art. 4 lett. g) del codice è:

Avv. / Dott. / Sig. _____ (* facoltativo)

ADOTTA IL SEGUENTE

DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

1. ELENCO DEI TRATTAMENTI DI DATI DELLO STUDIO LEGALE

- **(cod. 01)** dati personali dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 02)** dati personali 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;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 03)** dati personali 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;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 04)** dati personali 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;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 05)** dati personali dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 06)** dati personali 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;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 07)** 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;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 08)** dati giudiziari dei clienti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR n. 313/2002, o idonei a rivelare al qualità di imputato o indagato;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 09)** dati giudiziari di terzi, idonei a rivelare i provvedimenti di cui all'art. 3 DPR n. 313/2002, o idonei a rivelare al qualità di imputato o indagato;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 10)** 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;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 11)** dati sensibili dei clienti, dagli stessi forniti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 12)** dati sensibili di terzi, forniti dai clienti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

- **(cod. 13)** dati sensibili di clienti o terzi, comunque afferenti la vita sessuale.

( ) apporre una croce se questo tipo di trattamento viene effettuato
( ) apporre una croce se vi sono strutture esterne che concorrono al trattamento. In tal caso, indicare quali: _____

Gli strumenti utilizzati dagli incaricati per il trattamento sono:
( ) COMPUTER ( ) NOTEBOOK ( ) FAX ( ) CELLULARE ( ) _____

_____

_____

Per la descrizione degli strumenti utilizzati si rinvia alla sezione 2 del presente documento, nella parte in cui fa riferimento ai PROFILI DI AUTORIZZAZIONE degli incaricati.

Per la descrizione dei tipi d'interconnessione in uso si rinvia alla sezione 2 del presente documento, nella parte in cui fa riferimento al SISTEMA DI AUTORIZZAZIONE.

2. RUOLI, COMPITI E RESPONSABILITA'

SEZIONE LEGALE: AVVOCATO / I e PATROCINATORE / I

Comprende le operazioni di trattamento necessarie allo svolgimento di attività:

- giudiziale
- stragiudiziale
- consulenza legale
- _____

Elenco trattamenti: _____

SEZIONE PRATICANTATO: PRATICANTE / I

Comprende le operazioni di trattamento necessarie allo svolgimento di attività:

- archivio / ufficio
- assistenza alle udienze
- _____

Elenco trattamenti: _____

SEZIONE SEGRETERIA:

Comprende le operazioni di trattamento necessarie allo svolgimento di attività:

- archivio / ufficio
- amministrazione / rapporti di lavoro
- _____

Elenco trattamenti: _____

L'accesso ai dati personali e al loro trattamento con strumenti informatici da parte dei soggetti facenti parte delle varie SEZIONI dello Studio, è regolato in base alle seguenti misure minime di sicurezza:

i) SISTEMA DI AUTORIZZAZIONE

Il sistema di autorizzazione informatica utilizzato è: _____

SISTEMA OPERATIVO ( ) WINDOWS2000 ( ) WINDOWS NT ( ) MAC OS X ( ) LINUX _____

BREVE DESCRIZIONE

_____

_____

PROFILI DI AUTORIZZAZIONE

(Utilizzare specifiche lettere d'incarico per impartire istruzioni scritte agli incaricati – vedi all. 2)

AVVOCATI e PRATICANTI

Il/La Avv./Dott. _____

in qualità di avvocato/praticante presso lo Studio Legale _____

Qualifica: ( ) TITOLARE ( ) RESPONSABILE ( ) INCARICATO
è autorizzato al trattamento dei dati personali relativi a: (riprendere da elenco trattamenti – E' possibile identificarli attraverso il codice della sezione 1) e ad accedere alle seguenti aree:

Es: Aree di accesso: **BANCA DATI**: Ad es: NOMEFILE.DATABASE / DISCO RIGIDO SU PC/MAC (MARCA, MODELLO, UBICAZIONE, IN CONDIVISIONE) / **ARCHIVIO CARTACEO**: (UBICAZIONE, POSSESSO CHIAVI) / …

FINO AL 30/6/2005

DIPENDENTI

Il/La Sig./Sig.ra/Dott. _____

in qualità di dipendente presso lo Studio Legale _____

Qualifica: ( ) TITOLARE ( ) RESPONSABILE ( ) INCARICATO
è autorizzato al trattamento dei dati personali relativi a: (riprendere da elenco trattamenti – E' possibile identificarli attraverso il codice della sezione 1) e ad accedere alle seguenti aree:

Es: Aree di accesso: **BANCA DATI**: Ad es: NOMEFILE.DATABASE / DISCO RIGIDO SU PC/MAC (MARCA, MODELLO, UBICAZIONE, IN CONDIVISIONE) / **ARCHIVIO CARTACEO**: (UBICAZIONE, POSSESSO CHIAVI) / …

FINO AL 30/6/2005

---

ii) CREDENZIALI DI AUTENTICAZIONE

ASSEGNAZIONE CREDENZIALI DI AUTENTICAZIONE – AVVOCATI

Avv. _____ / anagrafica dell'avv.

Trattamento consentito ad esempio: ( ) **dati personali,** ( ) **sensibili,** ( ) **giudiziari**

UserID: _____ (riferimento ad es: iniziale nome / cognome MARIO ROSSI = MROSSI)

Aree di accesso: IN BASE AL TRATTAMENTO PER IL QUALE E' AUTORIZZATO

CODICI: _____

Data di attivazione: 30/6/2004 | Data di rinnovo: _____

ASSEGNAZIONE CREDENZIALI DI AUTENTICAZIONE – PRATICANTI

Dott. _____/ anagrafica praticante

Trattamento consentito ad esempio: ( ) **dati personali,** ( ) **sensibili,** ( ) **giudiziari**

UserID: _____ (riferimento ad es: iniziale nome / cognome MARIO ROSSI = MROSSI)

Aree di accesso: IN BASE AL TRATTAMENTO PER IL QUALE E' AUTORIZZATO

CODICI: _____

Data di attivazione: 30/6/2004 | Data di rinnovo: _____

ASSEGNAZIONE CREDENZIALI DI AUTENTICAZIONE – DIPENDENTI

Sig./Sig.ra. _____/anagrafica dipendente

Trattamento consentito: ( ) **dati personali,** ( ) **sensibili,** ( ) **giudiziari**

UserID: _____ (riferimento ad es: iniziale nome / cognome MARIO ROSSI = MROSSI)

Aree di accesso: IN BASE AL TRATTAMENTO PER IL QUALE E' AUTORIZZATO

CODICI: _____

Data di attivazione: 30/6/2004 | Data di rinnovo: _____

ASSEGNAZIONE CREDENZIALI DI AUTENTICAZIONE – TECNICI

Sig./Sig.ra./Dott. _____ (area tecnica) | Trattamento consentito: -

Aree di accesso: solo gestione tecnica

UserID: _____ | Password: ******

Data di attivazione: 30/6/2004 – Data di rinnovo: --

CREDENZIALI DI AUTENTICAZIONE - GARANZIE

Il Titolare garantisce la segretezza delle copie delle credenziali di autenticazione e indica

Il/La Avv./Sig./Sig.ra./Dott. _____ come incaricato della custodia della componente riservata delle credenziali di autenticazione, il/la quale informa tempestivamente gli incaricati di un eventuale intervento operato per necessità di operatività e sicurezza del sistema.

3. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

OPERATORI

Furto credenziali autenticazione:

> Sottrazione fraudolenta da parte di terzi — Rischio: ( ) alto ( ) medio ( ) basso

> Rivelazione o incauta esposizione delle credenziali — Rischio: ( ) alto ( ) medio ( ) basso

> — Rischio: ( ) alto ( ) medio ( ) basso

Azione: Rinnovo credenziali immediato

Carenza di consapevolezza, disattenzione o incuria:

> Pratiche incustodite — Rischio: ( ) alto ( ) medio ( ) basso

> Postazione informatica accessibile — Rischio: ( ) alto ( ) medio ( ) basso

> — Rischio: ( ) alto ( ) medio ( ) basso

Azione : Formazione in tema di sicurezza e rinnovo credenziali immediato

---

Comportamenti sleali o fraudolenti:

> Accesso abusivo al sistema informatico — Rischio: ( ) alto ( ) medio ( ) basso

> Sottrazione informazioni dati fascicoli — Rischio: ( ) alto ( ) medio ( ) basso

> — Rischio: ( ) alto ( ) medio ( ) basso

Azione: Denuncia e verifica integrità dati. Disattivazione credenziali.

STRUMENTI

Azione virus informatici:

> Infezione tramite posta elettronica — Rischio: ( ) alto ( ) medio ( ) basso

> Infezione tramite supporti (floppy ….) — Rischio: ( ) alto ( ) medio ( ) basso

> — Rischio: ( ) alto ( ) medio ( ) basso

Azione: Immediato ripristino situazione precedente all'evento. Antivirus o intervento manuale. Formazione su sicurezza informatica per soggetti Studio. Istruzioni (anche nella lettera di incarico)

Spamming:

> Ricevimento mail indesiderate — Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Installazione filtri anti-spam. Quando è possibile risalire alla fonte segnalazione al Garante.

Malfunzionamento e degrado strumenti:

> Componenti difettosi od obsoleti — Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Messa in sicurezza dei dati a rischio. Sostituzione strumenti.

Accessi esterni non autorizzati:

> Collegamento notebook alla rete informatica Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Predisposizione rete per riconoscimento IP autorizzati.

Intercettazione di informazioni in rete:

> Posta elettronica con / senza allegati Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Utilizzo crittografia, soprattutto per dati sensibili.

STUDIO LEGALE

Accessi non autorizzati a locali / reparti ad accesso ristretto:

> Archivio cartaceo Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Regolamento per orari, accesso e modalità

Asportazione e furto di strumenti contenenti dati:

> Asportazione computer Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Previsione software per crittografare hard disk. Ripristino da copia backup entro sette giorni su nuovo strumento.

Eventi distruttivi:

> Incendio locali Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Ripristino dati entro sette giorni. Backup dati affidato a ditte specializzate se tutti i supporti sono andati distrutti.

Guasto impianto elettrico:

> Procedura non corretta chiusura sessioni Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Attivazione automatica gruppi di continuità elettrici.

Errori umani gestione sicurezza fisica:

> Eliminazione fascicoli accidentale Rischio: ( ) alto ( ) medio ( ) basso

>

Azione: Ripristino situazione precedente. Ricostruzione fascicolo.

---

4. MISURE ADOTTATE PER GARANTIRE INTEGRITA' E DISPONIBILITA' DEI DATI

Queste misure riguardano tutti i tipi di trattamento dati descritti nella sezione 1.

1) PROTEZIONE FISICA DELLE AREE E DEI LOCALI
AI SENSI DELLA REGOLA 19.4 ALLEGATO B DEL CODICE

a) Sistema di protezione anti-intrusione / antincendio: _____

b) Sicurezza archivio cartaceo: _____

c) Eventuali aree facilmente accessibili: _____

d) Eventuali impianti di controllo accessi: _____

Responsabile controllo periodico efficienza: _____ Misure a) b) c) d)

2) PROTEZIONE INFORMATICA DEGLI STRUMENTI ELETTRONICI
AI SENSI DELLA REGOLA 19.4 ALLEGATO B DEL CODICE

e) Sistema operativo in uso: _____

f) Installazione software in grado di prevenire vulnerabilità e/o correggere difetti degli strumenti elettronici: _____

g) Software antivirus installato: _____ data ultimo aggiornamento: _____

h) Software firewall installato: _____ data ultimo aggiornamento: _____

Responsabile controllo periodico efficienza: _____ Misure e) f) g) h)

Le misure descritte alle lettere _____ sono già in essere.

Le misure descritte alle lettere _____ sono da adottare.

5. RIPRISTINO DISPONIBILITA' DEI DATI DISTRUTTI O DANNEGGIATI

Il salvataggio dei dati (c.d. back-up) viene effettuato con **frequenza settimanale** (regola 18 allegato B codice) attraverso la seguente procedura: _____

Le copie vengono conservate con le seguenti modalità: _____

Incaricato salvataggio dati:

Avv./Dott./Sig./Sig.ra _____

I supporti rimovibili utilizzati per il back-up vengono conservati con le seguenti modalità:

_____

Incaricato custodia supporti di back-up:

Avv./Dott./Sig./Sig.ra _____

La verifica della leggibilità del supporto viene effettuata: _____

_____

In caso di necessità, il ripristino avviene attraverso la seguente procedura:

_____

_____

6. DESCRIZIONE DELLE ATTIVITA' DI FORMAZIONE

Gli argomenti oggetto di formazione per gli incaricati del trattamento dei dati riguardano (19.6 allegato B del codice):

- Conoscenza dei rischi che incombono sui dati;
- Misure disponibili di attività fisiche, logiche e informatiche per prevenire eventi dannosi;
- Disciplina sulla protezione dei dati personali in rapporto alle relative attività;
- Profili di responsabilità in merito al trattamento dei dati.

Interventi formativi programmati:

Data: _____ Argomento (descrizione): _____

Relatore: _____

Data: _____ Argomento (descrizione): _____

Relatore: _____

e i relativi calendari.

N.B.: Indicare i soggetti interessati dai corsi di formazione (specificare se vi sono soggetti già formati o da formare durante l'anno su determinati argomenti):

_____

_____

_____

7. DATI PERSONALI AFFIDATI, IN CONFORMITA' AL CODICE, ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE

Il trattamento di dati personali (indicare se sensibili e giudiziari) relativo a _____ viene affidato a:

(persona fisica / persona giuridica) _____ (< inserire i dati relativi)

in data _____ fino a _____ (data / tempo indeterminato).

Il soggetto indicato ha rilasciato dichiarazione di conformità alle misure minime di sicurezza della sua struttura. Tale dichiarazione fa parte di un impegno assunto su base contrattuale. Il documento relativo è conservato presso questo Studio Legale.

8. TUTELA DEI DATI PERSONALI IDONEI A RIVELARE LO STATO DI SALUTE O LA VITA SESSUALE

I dati personali idonei a rivelare lo stato di salute o la vita sessuale vengono cifrati attraverso il software (o con le seguenti modalità): _____

e sono contenuti in: cartella / computer / banca dati separata.

I dati personali idonei a rivelare lo stato di salute o la vita sessuale vengono conservati in un apposito archivio separato situato in: _____ L'archivio è dotato di _____

Il presente documento programmatico della sicurezza è stato redatto, ai sensi dell'art. 34 del D. Lgs. 196/2003 e della regola 19 allegato B al codice da:
(QUALIFICA, NOME, COGNOME, TITOLARE/RESPONSABILE) _____
in data _____
E' composto di n. pag. _____

Rimane a disposizione degli organi competenti presso la struttura che lo ha redatto.

E' valido a tutti gli effetti di legge fino a: **31 marzo ….**

Milano, lì _____ Firma _____

ALLEGATO 1. INFORMATIVA AL CLIENTE

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, 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 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 _____ (indicare la persona fisica, l'associazione professionale o la società tra avvocati) con sede in

Responsabile del trattamento è il sig./dott.: _____ (da indicare se nominato).

Per ricevuta comunicazione

Data: _____ Firma: _____

ALLEGATO 2. LETTERA DI INCARICO

Il sottoscritto _____ in qualità di Titolare/Responsabile del trattamento dei dati dello Studio Legale _____ sito in _____

INCARICA

il Dr./sig./la sig.ra _____nato/a a _____ il _____ al trattamento dei dati (personali / sensibili / giudiziari : specificare anche con i codici del d.p.s.) nell'ambito delle funzioni di _____ (legale, praticantato, segreteria) che è chiamato/a a svolgere presso questo Studio.

A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- Il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare/Responsabile in generale ed elencate nel d.p.s.

Per ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:

a) divieto di comunicazione o diffusione dei dati senza la preventiva autorizzazione del Titolare/Responsabile;

b) l'accesso ai dati è autorizzato limitatamente all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;

c) la fase di trattamento dei dati dovrà essere preceduta dalla informativa al cliente in forma scritta e dal consenso di quest'ultimo al trattamento nei casi previsti dalla legge;

d) in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;

e) le proprie credenziali di autenticazione sono strettamente personali e devono rimanere riservate. Tali credenziali sono elencate nel documento programmatico sulla sicurezza dello Studio e univocamente associate all'incaricato al quale sono state fornite.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Qualsiasi altra istruzione può essere fornita dal Titolare che provvede anche alla formazione degli incaricati.

Per ogni altra misura qui non prevista si fa riferimento al documento programmatico sulla sicurezza adottato dallo Studio.

TRATTAMENTO CONSENTITO

a) raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

b) qualsiasi accesso e trattamento espressamente previsto dal profilo di autorizzazione associato e descritto nel d.p.s.;

c) qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

Data _____

L'incaricato

_____