Documento Programmatico sulla Sicurezza

Ai sensi dell'art. 34 e del disciplinare tecnico (allegato B)
del Codice in materia di Protezione dei Dati Personali D.Lgs. 196/03

(il presente fac simile deve essere compilato dal titolare di studio professionale composto dal singolo professionista che utilizzi strumenti informatici per il trattamento dei dati dei propri clienti/fornitori, necessari al regolare svolgimento del rapporto di prestazione d'opera professionale)

Il presente documento viene redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196, artt. da 33 a 36 (misure minime di sicurezza) nonché dal disciplinare tecnico contenuto nell'allegato B del citato decreto. In particolare:

- l'art. 34, comma 1, lettera g) del D.Lgs. 196/2003 prevede nel caso di trattamento di dati personali effettuato con strumenti elettronici l'obbligo della "*tenuta di un aggiornato documento programmatico sulla sicurezza*";
- il punto 19 dell'allegato B definisce le idonee informazioni necessarie per redigere il predetto documento, che di seguito viene più semplicemente definito DPS.

In particolare, sulla base delle regole previste dal disciplinare tecnico, il DPS è strutturato nelle seguenti sezioni:

A) ELENCO DEI TRATTAMENTI DI DATI PERSONALI

B) DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

C) ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

D) MISURE ADOTTATE E DA ADOTTARE

Il presente documento viene redatto da (*Titolare dello studio professionale)* nella sua qualità di titolare della sicurezza, che provvede e sottoscriverlo in calce.

Il DPS è inoltre corredato dalla seguente documentazione, che si riporta in allegato:

1) tabelle riassuntive e riepilogative di cui all'elenco che precede;

2) Dichiarazione di riservatezza e di conformità al D.Lgs. 196/03 del soggetto che gestisce la sicurezza informatica (manutenzione software e hardware);

A) ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Il Dott. (titolare dello studio) tratta i seguenti dati personali:

dati personali non sensibili dei fornitori, dei clienti, nonché degli eventuali dipendenti o collaboratori necessari al regolare svolgimento del rapporto di lavoro o di collaborazione,

Il Dott. (titolare dello studio) tratta i seguenti dati sensibili:

- dati sensibili dei clienti idonei a rivelare lo stato di salute o eventuali dati giudiziari;

Nella tabella 1.1 che segue si elencano schematicamente i trattamenti esistenti alla data di redazione e sottoscrizione del DPS, compresa ogni utile informazione idonea ad identificare inequivocabilmente il trattamento, la struttura dell'organismo all'interno della quale il trattamento viene eseguito, gli strumenti utilizzati nel trattamento.

1.1 INFORMAZIONI ESSENZIALI

DESCRIZIONE SINTETICA DEL TRATTAMENTO

Il Dott. (titolare dello studio) tratta i dati dei propri clienti e dei propri fornitori (e collaboratori esterni), necessari al regolare svolgimento del rapporto di lavoro professionale o di collaborazione.

NATURA DEI DATI TRATTATI

I dati trattati sono di natura personale e sensibile, infatti per le finalità di soddisfacimento del contratto d'opera professionale intercorrente tra il cliente ed il professionista, quest'ultimo può trattare anche dati concernenti lo stato di salute e/o dati giudiziari del cliente e, eventualmente, del dipendente/collaboratore.

DESCRIZIONE DEGLI STRUMENTI ELETTRONICI UTILIZZATI

I dati sono trattati attraverso l'inserimento in apposito software contenuto in (1 o più) elaboratori siti (indicare dove è/sono ubicatil il/i elaboratore/i) cui è possibile l'accesso al solo responsabile tramite credenziale di accesso riservata.

1.2 ELEMENTI ULTERIORI PER LA DESCRIZIONE DEGLI STRUMENTI ELETTRONICI (facoltativa da redigere solo in caso di effettiva esistenza di quanto descritto)

BANCA DATI

indicare l'esistenza di una banca dati (*data base o archivio informatico*) in cui sono contenuti i dati;

CUSTODIA SUPPOTI MEMORIZZAZIONE

indicare il luogo dove risiedono fisicamente i dati (*es. specifico elaboratore, server, centro di servizi, sito in …*), ovvero supporti utilizzati per le copie di sicurezza (*nastri, CD*);

TIPOLOGIA DI DISPOSITIVI DI ACCESSO

elenco e descrizione sintetica degli strumenti utilizzati per effettuare il trattamento (*tipi di hardware, palmare, telefono*);

TIPOLOGIA DI INTERCONNESSIONE

descrizione sintetica e qualitativa della rete che collega i dispositivi di accesso ai dati *(descrivere se i dati sono conservati su supporto hardware non collegato in rete, collegato solo in intranet, collegato con l'esterno)*.

B) DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Il Dott. (titolare dello studio) è l'unico autorizzato al trattamento dei dati.

C) ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

Descrivere i luoghi dove i dati vengono custoditi, come da esempio che segue: *"I dati vengono trattati presso la sede dello studio professionale il quale è ubicato es. in un condominio o in uno stabile autonomo in zona periferica/industriale/centrale/commerciale/residenziale, sito in…., dotato/non dotato di portoncino blindato o porta scorrevole a vetri, o porta con chiusura automatica, ecc… e con/senza videocitofono, con/ senza sorveglianza notturna, dotato/non dotato di sistema di allarme.*

Le singole stanze che compongono la sede sono dotate/non dotate di chiave, così come l'archivio, la stanza nella quale i dati vengono trattati/consultati, la biblioteca, ecc ….

La segreteria è situata in un locale ampio, nell'immediato ingresso della sede, dove in zona separata e opportunamente distanziata dai posti di lavoro è stata ricavata una sala di attesa per clienti, fornitori, rappresentanti, ecc…

La stanza archivio o segreteria, o altro è dotata/non dotata di cassaforte con chiusura a chiave o a combinazione, ecc…

Ogni ufficio è dotato di personal computer in rete è/non è connesso ad Internet/intranet con connessione ADSL. In segreteria o in altre stanze dello studio sono centralizzati i seguenti dispositivi:

- *stampante laser;*
- *fax a carta comune;*
- *fotocopiatrice;*
- *…."*

La totalità dei dati trattati possono essere conservati, alternativamente o contemporaneamente, in fascicoli riposti in schedari dotati di chiusura, in locali protetti, archiviati al termine della pratica, e tramite *personal computer* connessi in rete, seguendo le disposizioni minime di sicurezza.

D) MISURE ADOTTATE E DA ADOTTARE

A fronte dell'analisi dei rischi di cui alla precedente sezione C) di seguito si descrivono le misure di sicurezza adottate dallo studio.

INFORMAZIONI ESSENZIALI

MISURE PER IL CONTRASTO DEI RISCHI

descrivere sinteticamente le misure di sicurezza adottate o da adottare (*programmi antivirus, adozione di password personalizzate di accesso, archivi cartacei custoditi in armadi corazzati o con chiavi, misure di backup e di ripristino dei dati, ecc.*) nel caso di misura ancora da adottare indicare il tempo previsto per la messa in opera;

E) CIFRATURA DEI DATI O SEPARAZIONE DEI DATI IDENTIFICATIVI (per soli esercenti le professioni sanitarie o gli organismi sanitari)

INFORMAZIONI ESSENZIALI

TRATTAMENTO DI DATI

I dati protetti attraverso la cifratura riguardano quelli idonei a rivelare lo stato di salute o la vita sessuale del cliente.

PROTEZIONE SCELTA

riportare la tipologia di protezione scelta, su indicazione del codice o in base a specifiche considerazioni del titolare ad esempio cliente identificato secondo un codice alfanumerico, cui corrisponde una chiave per l'individuazione del nominativo;

TECNICA ADOTTATA

descrivere sinteticamente in termini tecnico o organizzativi, la misura adottata (*es. in caso di utilizzo della cifratura, le modalità di conservazione delle chiavi e le procedure di utilizzo*).

SCADENZE E AGGIORNAMENTI

Il DPS deve essere aggiornato ogni anno entro il **31 marzo**.

L'aggiornamento riguarda:

1) modalità di aggiornamento delle credenziali di autenticazione (ogni 3 mesi, da parte del titolare del trattamento dei dati);
2) individuazione del soggetto che procede alla manutenzione dei sistemi informatici o di altre modalità con le quali si assicura il buon funzionamento degli stessi;

3) attivazione di idonei strumenti per prevenire il rischio di danneggiamento dei software o degli hardware e quindi dei dati in essi contenuti, con cadenza almeno semestrale;
4) aggiornamento periodico dei software volti a prevenirne e a correggere i difetti, con cadenza semestrale;
5) modalità e cadenza di salvataggio dati e ripristino degli stessi.

Tali adempimenti vanno riportati nel DPS in sede in sede di aggiornamento annuale.
Per dare certezza della effettiva data, si suggerisce di far timbrare il DPS presso un ufficio postale o spedirlo a se stessi.