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 documento viene redatto in aderenza alle disposizioni di cui al 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 (TAB. 1.1 e TAB. 1.2)

B) DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' (TAB. 2)

C) ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (TAB. 3)

D) MISURE ADOTTATE E DA ADOTTARE (TAB. 4)

E) CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DATI (TAB 5)

F) PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI (TAB. 6)

G) TRATTAMENTI AFFIDATI ALL'ESTERNO (TAB. 7)

H) CIFRATURA DEI DATI O SEPARAZIONE DEI DATI IDENTIFICATIVI (per soli esercenti le professioni sanitarie o gli organismi sanitari) (TAB. 8)

Il presente documento viene redatto da *XXX* nella sua qualità di (*titolare/responsabile*) 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) (*riportare eventualmente in allegato fac-simili e carte di lavoro predisposte, quali ad esempio l'informativa, la lettera di incarico al responsabile o agli incaricati del trattamento, l'autorizzazione al trattamento da parte dell'interessato, ecc…)*

A) ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Il Consiglio degli Psicologi della Regione *XXX* (ovvero lo studio professionale *XXX* se si vuole adattare ai privati) tratta i seguenti dati personali:
(di seguito si forniscono alcuni esempi, relativi a situazioni comuni, soprattutto con riguardo ad un ordine professionale territoriale; l'elenco è ovviamente integrabile a seconda delle specifiche esigenze del soggetto obbligato)

- dati personali non sensibili dei clienti utenti, dei fornitori o di terzi ricavati o ricavabili da elenchi pubblici, albi professionali o camerali;
- dati personali non sensibili di soggetti terzi, forniti dai clienti utenti per l'espletamento degli incarichi affidati al titolare del trattamento;
- dati personali non sensibili dei dipendenti e dei collaboratori, necessari al regolare svolgimento del rapporto di lavoro o di collaborazione, nonché quelli affidati al datore di lavoro per esigenze di natura bancaria.

Il Consiglio degli Psicologi della Regione *XXX* (ovvero lo studio professionale *XXX* se si vuole adattare ai privati) tratta i seguenti dati sensibili (*seguono esempi*):

- dati sensibili del personale dipendente, idonei a rivelare ……. (*per esempio stato di salute o vita sessuale o dati giudiziari*);
- dati sensibili degli *iscritti/clienti/utenti*, idonei a rivelare ……. (*per esempio stato di salute o vita sessuale o 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. Per questi ultimi, ove necessario, sono indicati ulteriori elementi necessari alla miglior individuazione di quanto tecnicamente utilizzato a supporto del singolo trattamento.

1.1 INFORMAZIONI ESSENZIALI (TAB. 1.1)

DESCRIZIONE SINTETICA DEL TRATTAMENTO indicare la finalità perseguita dal trattamento e le categorie di persone cui i dati si riferiscono.

NATURA DEI DATI TRATTATI indicare se tra i dati trattati ci sono dati sensibili o;

STRUTTURA DI RIFERIMENTO indicare la struttura e sottostruttura, se esistente, all'interno della quale viene effettuato il trattamento (*es. studio privato, struttura pubblica- ufficio*);
STRUTTURE CONCORRENTI AL TRATTAMENTO se il trattamento, per essere completo, ha bisogno di strutture esterne concorrenti è opportuno indicare la struttura dove primariamente viene effettuato il trattamento dei dati e quelle concorrenti;
DESCRIZIONE DEGLI STRUMENTI ELETTRONICI UTILIZZATI indicare la tipologia di strumenti elettronici impiegati per la raccolta dei dati (*elaboratori in rete, non in rete, portatili, palmari, fissi, utilizzo di internet o qualsiasi sistema informativo anche più complesso*).

La tabella 1.2 può essere adottata nel caso di strutture particolarmente complesse che necessitino di ulteriori specificazioni circa le modalità di trattamento.

1.2 ELEMENTI ULTERIORI PER LA DESCRIZIONE DEGLI STRUMENTI ELETTRONICI

(TAB. 1.2)

IDENTIFICATIVO DEL TRATTAMENTO ad ogni trattamento può essere attribuito un codice che lo identifichi, se ritenuto utile;
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*), ovvero supporti utilizzati per le copie di sicurezza (*nastri, CD*);
TIPOLOGIA DI DISPOSITIVI DI ACCESSO elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento (*pc, palmare, telefono*);
TIPOLOGIA DI INTERCONNESSIONE descrizione sintetica e qualitativa della rete che collega i dispositivi di accesso ai dati.

B) DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' (TAB. 2)

Il Consiglio degli Psicologi della Regione *XXX* è già dotato di una pianta organica e di un mansionario che vengono allegati al presente documento sub *X*.
Considerando quindi le risorse a disposizione della struttura, nella tabella 2.1 sono specificatamente riportate le informazioni in materia di sicurezza del trattamento dei dati.

INFORMAZIONI ESSENZIALI

STRUTTURA indicare come è composta la struttura nella quale vengono trattati i dati (*vedi punto 1.1-Struttura*);
TRATTAMENTI EFFETTUATI DALLA STRUTTURA indicare i trattamenti effettuati;
COMPITI E RESPONSABILITA' descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza (*es. acquisizione caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa dei data base*);

C) ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (TAB. 3)

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.

È necessario ed opportuno, a questo punto, descrivere i luoghi dove i dati vengono custoditi, come da esempio che segue: "*Le sede del Consiglio degli Psicologi della Regione XXX ove vengono trattati i dati, è ubicato es. un condominio in zona periferica/industriale/…, o in un singolo stabile sito in, dotato di portoncino blindato o porta scorrevole a vetri, o porta con chiusura automatica, ecc… e con videocitofono, con o senza sorveglianza notturna, dotato di sistema di allarme.*
Le singole stanze che compongono la sede sono dotati di chiave, così come l'archivio, la stanza EDP, 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 di cassaforte con chiusura a chiave o a combinazione, ecc…
Ogni ufficio è dotato di personal computer in rete e connesso ad Internet con connessione ADSL. In segreteria sono centralizzati i seguenti dispositivi:

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

E' stata compiuta l'analisi dei rischi, avendo attenzione alla tipologia degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali, nonché all'impatto sulla

sicurezza dei dati, in relazione a ciascun evento e alla gravità e probabilità stimata dell'evento steso. Per ciascun eventi probabile, si è ipotizzato naturalmente la contromisura adottata o da adottare.

INFORMAZIONI ESSENZIALI

COMPORTAMENTO DEGLI OPERATORI indicare se un comportamento degli operatori improntato a: sottrazione delle credenziali di autenticazione, carenza di consapevolezza disattenzione o incuria, comportamenti sleali o fraudolenti, errore materiale, possa incidere con gravità alta, media o bassa, sulla sicurezza di dati anche in relazione alla rilevanza e alla probabilità stimata dell'evento;

EVENTI REALTIVI AGLI STRUMENTI indicare se i seguenti eventi possano incidere con gravità alta, media o bassa, sulla sicurezza di dati anche in relazione alla rilevanza e alla probabilità stimata dell'evento: azione di virus informatici, *spamming* o tecniche di sabotaggio, malfunzionamento, indisponibilità o degrado degli strumenti, accessi esterni non autorizzati, intercettazione di informazioni in rete;

EVENTI RELATIVI AL CONTESTO FISICO AMBIENTALE indicare se i seguenti eventi possano incidere con gravità alta, media o bassa, sulla sicurezza di dati anche in relazione alla rilevanza e alla probabilità stimata dell'evento: ingressi non autorizzati ai locali/aree ad accesso ristretto, sottrazione di strumenti contenenti dati, eventi distruttivi naturali o artificiali nonché dolosi o accidentali o dovuti ad incuria, guasti a sistemi complementari (*impianto elettrico, idrico*), errori umani nella gestione della sicurezza fisica.

D) MISURE ADOTTATE E DA ADOTTARE (TAB. 4)

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

4.1 INFORMAZIONI ESSENZIALI (TAB. 4.1)

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

Si suggerisce come esempio:

Misura 1. Antivirus. Ogni singolo computer è dotato di dispositivo antivirus, che viene aggiornato con funzione automatica e con scansione per ogni aggiornamento antivirus, e in ogni caso almeno

settimanalmente, in orario compatibile con il fatto che il computer non sia spento (in questo caso la scansione avverrà alla successiva accensione).

Misura 2. Firewall. Sul server è stato installato firewall con le seguenti caratteristiche: …

Misura 3. Backup. 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 armadio chiuso a chiave e protetto da agenti ignifughi, 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; una volta effettuato e verificato un backup, deve essere distrutto il cd rom precedente.

Misura 4. Screensaver. Tutti gli utilizzatori di strumenti elettronici non devono lasciare incustodito, o accessibile, lo strumento stesso. A tale riguardo, per evitare errori e dimenticanze, è stato predisposto lo screensaver automatico dopo … minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.

Misura 5. Autenticazione informatica. Tale misura è stata adottata dotando ciascun incaricato di una password di almeno 8 caratteri. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né alla società. 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 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.

Misura 6. Archiviazione. Si è disposto che non siano lasciati 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.

Misura 7. Stampe centralizzate. Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato dall'interessato o consegnato allo stesso.

Misura 8. Fax. I fax sono ricevuti su carta normale, e quindi è evitato il deterioramento tipico della carta chimica. I documenti arrivano in zona protetta, accessibile solo dagli incaricati dell'area della segreteria, con la parte scritta verso il basso per evitare di rimanere in vista incidentalmente.

Misura 9. Archivio. Il locale destinato all'archivio è sempre chiuso a chiave. L'incaricato preposto dovrà controllare l'accesso all'archivio. Fuori dall'orario di lavoro l'accesso all'archivio è consentito esclusivamente previa registrazione.

Misura 10. Distruzione documenti. Si è data istruzione che il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia riposto negli appositi sacchi di plastica, previo passaggio nelle apposite macchine taglia documenti (in dotazione almeno in misura di uno per ciascun ufficio)

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.

Misura 11. Eventi naturali. La società ha provveduto ad adottare le disposizioni di sicurezza stabilite dalla L. 626/94.

DESCRIZIONE DEI RISCHI per ciascuna misura indicare i rischi che si intendono contrastare (*es. programma antivirus – azione di virus informatici, password personalizzate di accesso – accessi esterni non autorizzati, ecc*);

TRATTAMENTI INTERESSATI indicare i trattamenti interessati per ciascuna delle misure adottate, nel caso in cui ciò sia possibile;

STRUTTURA O PERSONE ADDETTE ALL'ADOZIONE indicare la struttura o le persone responsabili o preposte all'adozione delle misure indicate.

4.2 ULTERIORI ELEMENTI PER LA DESCRIZIONE ANALITICA DELLE MISURE DI SICUREZZA (TAB. 4.2)

Oltre alle informazioni sopra riportate è facoltà dei titolari della strutture più complesse dove vengono trattati i dati compilare, per ciascuna misura di sicurezza, una scheda analitica contenete un maggior numero di informazioni. A titolo di esempio in queste schede si possono indicare: il tipo di misura adottata, la minaccia che si intende contrastare, le informazioni relative alla responsabilità e all'attuazione, gli ambiti cui si applica (fisici o logici).

E) CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DATI (TAB 5)

Oltre alla procedura di backup l'Ente ha approntato la seguente procedura di "*disaster recovery*", vale a dire di ripristino della disponibilità dei dati.

Si premette che ci si avvale anche della consulenza informatica della società ……., come risulta anche dalla lettera di assunzione di incarico sottoscritta in data ……

Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici:

1. deve essere avvertito il titolare del trattamento dei dati e l'incaricato che ha in custodia il CD ROM di back up nonché i CD ROM contenenti i vari software installati sugli strumenti elettronici;
2. ci si deve rivolgersi immediatamente al tecnico manutentore del consulente informatico sollecitandone al più presto l'assistenza;
3. ciascun incaricato deve provvedere ad inventariare nella maniera più precisa possibile il lavoro svolto dal momento dell'ultimo back up al momento della rottura irreversibile;

4. si devono reinstallare i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nel CD ROM di back up;
5. si deve provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
6. 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.

5.1 INFORMAZIONI ESSENZIALI (TAB. 5.1)

BANCA DATI/DATA BASE/ARCHIVIO indicare quale tra questi ha copie di salvataggio dei dati contenuti;

CRITERI E PROCEDURE descrivere la tipologia del salvataggio dei dati e la frequenza (es. supporto cd ogni settimana);

MODALITA' DI CUSTODIA DELLE COPIE indicare il luogo fisico in cui sono custodite le copie dei dati;

PIANIFICAZIONE DELLE PROVE DI RIPRISTINO indicare i tempi previsti per i test di efficacia delle procedure di salvataggio/ripristino dei dati

5.2 ULTERIORI ELEMENTI (TAB. 5.2)

facoltativamente si può indicare le modalità di custodia delle copie dei dati e la struttura o la persona incaricata di effettuare il salvataggio e di controllarne l'esito.

F) PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI (TAB. 6)

Nell'ambito delle procedure di tutela della sicurezza dei dati trattati dallo studio si è proceduto a stila re il piano dell'impegno formativo che si prevede di sostenere in attuazione della normativa sulla privacy, secondo la tabella che segue.

INFORMAZIONI ESSENZIALI

DESCRIZIONE SINTETICA DEGLI INTERVENTI FORMATIVI descrivere sinteticamente gli obiettivi e le modalità dell'intervento formativo (*es. ingresso in servizio, cambiamento di mansioni, introduzione nuovi supporti informatici ecc.*);

CLASSI DI INCARICO O TIPOLOGIE DI INCARICATI INTERESSATI individuare le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati;

TEMPI PREVISTI indicare i tempi previsti per lo svolgimento degli interventi formativi.

G) TRATTAMENTI AFFIDATI ALL'ESTERNO (TAB. 7)

In quest'ultima sezione vengono fornite, con l'ausilio della successiva tabella 7.1, tutte le indicazioni necessarie ad identificare i dati trattati all'esterno, nonché i soggetti coinvolti.
Si premette che è stata predisposta idonea documentazione rilasciata dai soggetti cui le varie attività sono affidate dalla quale risulta:

- che il terzo dichiara di essere consapevole che i dati da lui trattati nell'espletamento dell'incarico ricevuto sono dati personali e, come tali, sono soggetti alla disciplina di cui al D.Lgs. 196/2003 (Codice per la protezione dei dati personali);
- che il terzo dichiara di ottemperare agli obblighi previsti dal predetto D.Lgs. 196/2003;
- che il terzo dichiara di adottare ogni istruzione ricevuta dal titolare del trattamento;
- che il terzo si impegna a relazionare il titolare in ordine alle misure di sicurezza da lui adottate, notiziando il committente circa le situazioni di pericolo per i dati in cui potrebbe imbattersi;
- che il terzo dichiara di riconoscere il diritto del committente alla verifica periodica dell'applicazione delle norme di sicurezza adottate.

INFORMAZIONI ESSENZIALI
DESCRIZIONE DELL'ATTIVITA' ESTERNALIZZATA indicare sinteticamente l'attività affidata all'esterno;
TRATTAMENTI DI DATI INTERESSATI indicare i trattamenti di dati, sensibili o giudiziari, effettuati nell'ambito della predetta attività;
SOGGETTO ESTERNO indicare la società, l'ente o il consulente esterno cui è stata affidata l'attività,
DESCRIZIONE DEI CRITERI il soggetto esterno cui è affidato tutto o parte del trattamento dei dati, deve dare assicurazioni, anche per iscritto, sui criteri con i quali tratterà i dati dando assicurazioni, anche per contratto, di trattare i dati: ai soli fini dell'espletamento dell'incarico ricevuto, i osservanza alle norme del Codice per la protezione dei dati personali; nel rispetto delle istruzioni specifiche ricevute, relazionando periodicamente il titolare.

H) CIFRATURA DEI DATI O SEPARAZIONE DEI DATI IDENTIFICATIVI (per soli esercenti le professioni sanitarie o gli organismi sanitari) (TAB. 8)

INFORMAZIONI ESSENZIALI

TRATTAMENTO DI DATI indicare e descrivere i dati oggetto di questa specifica protezione (dati sensibili di natura sanitaria);

PROTEZIONE SCELTA riportare la tipologia di protezione scelta, su indicazione del codice o in base a specifiche considerazioni del titolare;

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*).

Il DPS deve contenere le informazioni sinteticamente indicate fin qui, in base alla natura del soggetto titolare del trattamento (Ente pubblico o libero professionista) ovvero alla complessità della struttura nella quale i dati vengono trattati. Per privati professionisti con strutture semplici la redazione sarà estremamente semplificata, dovendo riportare solo alcune delle informazioni richieste, per realtà più complesse le informazioni dovranno essere maggiormente specificate. Il DPS deve essere aggiornato entro il 30 marzo di ogni anno. In sede di aggiornamento potranno essere inserite maggiori informazioni e affinato il suo contenuto.