DPS e Protezione dei dati

Sonia Volpe – Lessicom srl

il DPS

Redazione periodica del DPS (Documento Programmatico sulla Sicurezza)
Riferimenti normativi: Codice in materia di protezione dei dati personali – art. 34 e Allegato B, regola 19, del d.lg. 30 giugno 2003, n. 196

1.
Il **Documento Programmatico** sulla **Sicurezza** (DPS) **deve essere redatto entro il 30 giugno 2006 ed aggiornato entro il 31 marzo di ogni anno.**

Il DPS ha lo **scopo di delineare** il quadro delle misure di sicurezza, organizzative, fisiche e logiche da adottare per la protezione dei dati personali trattati contro il verificarsi di qualsiasi evento dannoso o pericoloso.
Il DPS **può essere predisposto internamente** o avvalendosi della consulenza di specialisti esterni allo Studio.

Il DPS deve essere **redatto secondo le linee guida** specificate al punto 19 Allegato B) del Codice 196/03 e cioè:

ART. 19.1
- ✓ elencare le banche dati presenti in Studio specificando le categorie di soggetti interessati e le finalità della raccolta
- ✓ specificare le modalità del trattamento
- ✓ elencare gli strumenti elettronici utilizzati (facoltativo)

ART. 19.2
- ✓ elencare i soggetti coinvolti nel trattamento specificando i compiti e le responsabilità

ART. 19.3
- ✓ elencare i rischi che incombono sui dati specificando il livello (basso, medio, alto)

ART. 19.4
- ✓ elencare le misure adottate per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali
- ✓ descrivere le modalità per il trattamento senza strumenti elettronici

ART. 19.5
- ✓ descrivere le modalità di back-up

ART. 19.6
- ✓ descrivere un piano di formazione ed informazione degli incaricati

ART. 19.7
- ✓ elencare i soggetti esterni a cui vengono inoltrati dati sensibili oggetto di trattamento a mezzo di strumenti elettronici e verificare che abbiano adottato le misure minime di sicurezza e redatto il DPS

ART. 19.8
- ✓ elencare i trattamenti dei dati sensibili oggetto di specifica protezione (stato di salute e vita sessuale)
- ✓ indicare la tipologia di protezione adottata (cifratura o separazione di dati personali e sensibili)
- ✓ descrivere sinteticamente in termini tecnici ed organizzativi la misura adottata

Il DPS non deve essere inviato al Garante, ma conservato in Studio per esibirlo a fronte di una verifica da parte degli organismi di controllo preposti (Garante o GdF).
Per **ottenere il requisito della data certa** in sede di prima stesura e per i successivi aggiornamenti, è sufficiente alternativamente:

- far apporre il timbro datario presso un ufficio postale direttamente sul documento (**autoprestazione**)
- redigere un'**autocertificazione** in cui si dichiara di aver redatto il DPS entro una determinata data

2. regime sanzionatorio

Il regime sanzionatorio è molto pesante.
Le sanzioni non sono graduate rispetto all'effettiva gravità della violazione, specie in caso di inosservanza di semplici aspetti formali.
Non viene prevista alcuna differenziazione in relazione alla natura ed alla dimensione del soggetto sanzionato.

- L'omissione dell'informativa è punita con il pagamento di una somma da 3.000,00 € a 18.000,00 € e, nei casi di dati sensibili o giudiziari, da 5.000,00 € a 30.000,00 €.
- Il trattamento illecito di dati personali è punito con una reclusione che varia con la gravità del reato.
- L'omessa adozione delle misure minime di sicurezza è un illecito penale punito con l'arresto sino a 2 anni o con l'ammenda da 10.000,00 € a 50.000,00 €.

Le violazioni della disciplina sulla privacy sono inoltre fonte di responsabilità civile per danni: il trattamento dati viene qualificato dal Codice come esercizio di attività pericolosa (art. 2050 del Codice Civile).
Il titolare del trattamento può dunque discolparsi e liberarsi dalla responsabilità civile solamente dimostrando di avere adottato ogni misura idonea ad evitare il danno.

3. riferimenti utili

Decreto Legislativo 30 giugno 2003, n. 196
"Codice in materia di protezione dei dati personali", Gazzetta Ufficiale n. 174 del 29 luglio 2003, Supplemento Ordinario n. 123
Reperibile sul sito www.garanteprivacy.it

Scheda informativa del Garante datata 13.05.05
"Prime riflessioni sui criteri di redazione del Documento Programmatico sulla Sicurezza (DPS)"
Reperibile sul sito www.garanteprivacy.it

Guida operativa per redigere il Documento Programmatico sulla Sicurezza (DPS) del 11.06.04
Reperibile sul sito www.garanteprivacy.it

la Privacy

Il tema della protezione dei dati si inserisce nel più ampio contesto della **tutela aziendale** ed è finalizzato a dotare l'azienda di idonee garanzie contro le minacce endogene (interne) ed esogene (esterne).

Il Decreto Legislativo 30 giugno 2003 n. 196 – "Codice in materia di protezione dei dati personali", entrato in vigore il 01 gennaio 2004, abroga esplicitamente la quasi totalità dei precedenti provvedimenti in materia di privacy e si applica al trattamento di dati personali da chiunque effettuato nel territorio dello Stato.

Gli assunti fondamentali sono i seguenti:

- ✓ **chiunque ha diritto alla protezione dei dati personali che lo riguardano**
- ✓ **il trattamento deve svolgersi nel rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati (quindi, anche dei pazienti) con particolare riferimento alla riservatezza, all'identità personale ed alla protezione dei dati.**

Chiunque tratti dati (quindi, anche lo Studio Odontoiatrico) deve adempiere a tutte le prescrizioni e predisporre le previste misure minime di sicurezza.

Obiettivo comune di tutte le misure di sicurezza è la **riduzione dei rischi**.
A fini cognitivi e di valutazione complessiva, i rischi possono essere **classificati** in:

1. **interni** (connessi all'attività dei dipendenti dell'azienda)
2. **esterni** (connessi all'attività di terzi)
3. **ambientali** (relativi a eventi di grande portata quali incendi, terremoti, allagamenti)
4. **organizzativi** (connessi a responsabilità non correttamente assegnate, sottovalutazione dei rischi)
5. **colposi** (causati da ignoranza, leggerezza, incuria)
6. **dolosi** (causati da volontà di arrecare danno).

La **riduzione del rischio** è finalizzata al raggiungimento degli **obiettivi** di:

- **riservatezza** (limitare al massimo la fruizione da parte di soggetti non autorizzati)
- **integrità** (limitare al massimo i rischi di cancellazioni o modifiche a causa di interventi esterni o malfunzionamenti di hardware e software)
- **disponibilità** (garantire al massimo la fruizione da parte di soggetti autorizzati).

DEFINIZIONI UTILI:

1. trattamento

"qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di mezzi elettronici", concernenti:

- raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione (inserire il dato in un luogo o contesto organizzato secondo determinati criteri, farlo proprio e utilizzarlo)
- blocco (conservare il dato con sospensione temporanea di ogni altra operazione di trattamento)
- comunicazione (portare il dato a conoscenza di uno o più soggetti determinati, diversi dall'interessato, anche mediante la loro messa a disposizione o consultazione)
- diffusione (portare il dato a conoscenza di soggetti indeterminati, diversi dall'interessato, anche mediante la loro messa a disposizione o consultazione)
- cancellazione (eliminare il dato, ma non distruggerlo totalmente)
- distruzione (eliminare il dato totalmente).

Il trattamento concerne quindi l'INTERA VITA del dato personale e si configura sia che le operazioni sussistano singolarmente, sia cumulativamente.

Il trattamento può essere:

- non automatizzato (supporti esclusivamente cartacei)
- automatizzato (elaboratori stand alone o collegati in rete)
- non automatizzato + automatizzato (supporti cartacei + elaboratori stand alone o collegati in rete)

2. dati

"informazioni sull'interessato" suddivisi in:

- **anonimi**

non associabili ad un interessato identificato o identificabile (in origine o in seguito a trattamento).

- **personali**

atti a identificare direttamente (nome, cognome, ragione sociale) o indirettamente (codice fiscale, numero di targa, registrazioni visive o sonore, impronte digitali, caratteristiche genetiche) una persona fisica, giuridica o un ente.

- **sensibili**

atti ad individuare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesioni a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico politico o sindacale**, stato di salute**, vita sessuale.

- **giudiziari**

atti ad individuare la presenza di provvedimenti giudiziari (casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, qualità di imputato o di indagato).

I dati devono essere:

- **trattati** in modo lecito e secondo correttezza
- **raccolti** e registrati per scopi determinati
- **esatti**, **aggiornati**, **pertinenti**, **completi** e **non eccedenti** rispetto alle finalità per le quali sono raccolti o successivamente trattati
- **conservati** in forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati trattati in violazione della norma non sono utilizzabili.

3. soggetti

I **soggetti coinvolti** nella concreta attuazione delle misure minime di sicurezza sono:

- **interessato**

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

- **titolare**

"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"

Titolare è il titolare di studio odontoiatrico.

Per gli studi associati o società, il titolare è la persona giuridica (lo studio associato o la società), non i singoli professionisti.

- **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".
Il responsabile deve essere nominato tra i soggetti che, per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
Il responsabile procede al trattamento attenendosi alle istruzioni del titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni e delle proprie istruzioni.
I compiti affidati al responsabile devono essere analiticamente specificati per iscritto dal titolare il quale vigila sull'osservanza delle istruzioni impartite.
Nello studio odontoiatrico monoprofessionale, titolare e responsabile possono coincidere.

- **incaricato**

"La persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile".
L'ambito del trattamento ed i compiti affidati all'incaricato devono essere analiticamente specificati per iscritto dal titolare (o dal responsabile, se designato) il quale vigila sull'osservanza delle istruzioni impartite.

Nello studio odontoiatrico incaricati sono i medici collaboratori, gli igienisti, il personale assistente e di segreteria

4. adempimenti

- **informativa agli interessati**

Chiunque tratti dati, sia con mezzi elettronici, sia manuali è tenuto a renderne informazione all'interessato al momento della raccolta e comunque non prima della comunicazione degli stessi a soggetti terzi.
Più specificamente, l'informativa deve contenere:

a. l'**elenco dei diritti** dell'interessato
b. le **specifiche** del trattamento (finalità e modalità)
c. la **natura del conferimento** (obbligatoria, facoltativa)
d. le **conseguenze** di un eventuale rifiuto
e. l'**indicazione dei soggetti** a cui possono essere comunicati i dati.

- **raccolta del consenso**

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.
Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.
Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le necessarie informazioni

Il consenso al trattamento dei dati personali può essere reso in qualunque forma, quello al trattamento dei dati sensibili necessariamente in forma scritta.

5. misure minime per il trattamento dei dati

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

6. Trattamenti con strumenti elettronici

6.1 sistema di autenticazione informatica

codice per l'identificazione dell'incaricato (**user id**) associato ad una parola chiave riservata (**password**) conosciuta solamente dal medesimo

o

dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato, eventualmente associato ad un codice identificativo o ad una parola chiave

o

caratteristica biometrica dell'incaricato eventualmente associata ad un codice identificativo o ad una parola chiave

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

- La **parola chiave è composta da almeno 8 caratteri** e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- La **parola chiave è modificata dall'incaricato al primo utilizzo** e, **successivamente almeno ogni 6 mesi.** In caso di trattamento di dati sensibili e giudiziari la parola chiave è modificata **almeno ogni 3 mesi**.
- Il **codice per l'identificazione non può essere assegnato ad altri incaricati**, neppure in tempi diversi.
- Le **credenziali di autenticazione non utilizzate da almeno 6 mesi sono disattivate**, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- Le **credenziali sono disattivate anche in caso** di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- Sono **impartite istruzioni agli incaricati** per non lasciare incustodito ed accessibile lo strumento elettronico durante una sessione di trattamento (**screen saver**).

Quando l'accesso ai dati ed agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza ed individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato (custode delle password).

6.2 sistema di autorizzazione

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione **(in sede di redazione del dps).**

6.3 protezione

I dati personali sono protetti contro il rischio di intrusione mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale **(firewall e antivirus).**

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici ed a correggerne i difetti sono effettuati almeno annualmente.

In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale (**sistema operativo**).

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale (**back up**).

7. trattamenti senza strumenti elettronici

Agli incaricati sono **impartite istruzioni scritte** finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento degli atti e dei documenti contenenti dati personali.

Quando gli atti ed i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate.

L'**accesso agli archivi** contenenti dati sensibili o giudiziari è controllato **(chiusura a chiave, codifica numerica).**

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate