

**DOCUMENTO PER LA SICUREZZA  
DEI TRATTAMENTI DI DATI PERSONALI  
EFFETTUATI CON STRUMENTI ELETTRONICI**

(ART. 34 E REGOLA 19 DELL'ALLEGATO B DEL CODICE  
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI)

Effettuati da:

Ragione sociale: .....

Indirizzo: .....

Sede operativa: .....

Partita IVA: .....

Attività: .....

Telefono: .....

**Annotazione**

*Quanto riportato in questo documento è soggetto ad aggiornamento, la cui scadenza è fissata entro il 31 marzo di ogni anno.*

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
**Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196**

---

## 1. SCOPO DEL DOCUMENTO

Il presente documento, in ottemperanza alle prescrizioni del D.Lgs. n. 196/2003 (“Codice della Privacy”), individua le linee guida generali, le azioni e le misure per il trattamento dei dati personali in condizione di sicurezza con la finalità di ridurre al minimo, con riferimento alla tipologia dei dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

Il sistema informatico descritto nel presente documento deve ritenersi sicuro in quanto persegue la **disponibilità**, l'**integrità** e l'**autenticità**, nonché la **riservatezza** dell'informazione e dei servizi per il trattamento, attraverso *l'attribuzione di specifici incarichi*, la *certificazione delle fonti di provenienza dei dati* e le *istruzioni per le persone autorizzate ad effettuare i trattamenti*.

La stesura del presente documento è aderente alle seguenti linee guida:

1. analisi dello stato dell'organizzazione attraverso l'identificazione e distinzione delle responsabilità delle figure soggettive coinvolte nel trattamento; l'identificazione, l'inventario e l'analisi dell'hardware, del software e delle banche dati;
2. l'individuazione e la valutazione del rischio
3. l'individuazione delle misure preventive e correttive
4. l'individuazione di istruzioni agli incaricati e la previsione di un programma formativo

## 2. ORGANIGRAMMA DELLA SICUREZZA DEI TRATTAMENTI

a) **Titolare del trattamento dei dati** (titolare dell'impresa odontotecnica):

\_\_\_\_\_

b) **Responsabile del trattamento** (ove nominato):

\_\_\_\_\_

c) **Incaricati dei trattamenti di dati personali**:

1) \_\_\_\_\_

2) \_\_\_\_\_

3) \_\_\_\_\_

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
**Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196**

---

**3. INVENTARIO DEI COMPUTER, DEI PROGRAMMI E DELLE BANCHE DATI (elettroniche e/o su carta)**

a) Identificazione e inventario dei **computer**

<i><b>Modello di computer</b></i>	<i><b>numero di matricola computer</b></i>
Modello: .....	n° .....
Modello: .....	n° .....

b) Identificazione, inventario ed analisi dei **programmi** aziendali

<i><b>Nome programma</b></i>	<i><b>Tipo di trattamento effettuato</b></i>
Es.: programma di contabilità	Gestione contabile dei dati aziendali

c) Identificazione, inventario ed analisi delle **banche dati**

<i><b>Contenuto della banca dati</b></i>	<i><b>Finalità del trattamento</b></i>	<i><b>Dati sensibili</b></i>	<i><b>Supporto impiegato</b></i>
Es.: banca dati dei clienti o dei fornitori	Gestione amministrativa e fatturazione		

d) Identificazione, inventario ed analisi dei **supporti cartacei**

<i><b>Contenuto della banca dati</b></i>	<i><b>Finalità del trattamento</b></i>	<i><b>Dati sensibili</b></i>
Es.: Prima nota	Gestione amministrativa	

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
**Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196**

---

**4. ELENCO PER L'INDIVIDUAZIONE E LA VALUTAZIONE DEI RISCHI**

<i>Risorsa</i>	<i>Fattore di rischio</i> <sup>(2)</sup>	<i>R</i> <sup>(1)</sup>	<i>Misura adottata</i> <sup>(2)</sup>
<b>Risorse umane</b>	1. Turn-over		
	2. Assenze		
	3. Ignoranza procedurale		
	4. ...		
<b>Computer</b>	5. Guasto tecnologico		
	6. Danneggiamento		
	7. Incendio		
	8. Uso illegittimo		
	9. Furto		
	10. Assistenza		
	11. Virus		
	12. Impossibilità d'uso		
	13. Obsolescenza		
	14. Interruzione d'uso		
<b>Programmi</b>	15. Virus		
	16. Danneggiamento		
	17. Copia abusiva		
	18. Validità licenza d'uso		
	19. Impossibilità d'uso		
	20. Interruzione d'uso		
	21. Furto		
	22. Obsolescenza		
	23. Abilitazione all'accesso		
	24. Manutenzione		
<b>Dati</b>	25. Integrità logica		
	26. Intercettazione		
	27. Modifica non controllata		
	28. Impossibilità di ripristino		
	29. Cancellazione		
	30. Virus		
	31. Comunicazione illegittima		
	32. Diffusione illegittima		
	33. Distruzione		
	34. Mancanza documentazione		
<b>Trasmissioni</b>	35. Interruzione trasmissione		
	36. Malfunzionamento		
	37. Intercettazione volontaria		

<sup>(1)</sup> **R** deve essere espresso con la variabile di valutazione: **A = Alto**; **M = Medio**; **B = Basso**

<sup>(2)</sup> Individuare le misure, utilizzando l'unito elenco, riportando volta per volta la relativa numerazione.

## **5. ELENCO DELLE MISURE DI SICUREZZA**

### **1. MISURE MINIME** (*Disciplinare tecnico di cui all'Allegato B, art. 36 D.Lgs. 196/2003*)

- 1.1 Definizione di credenziali di autenticazione  
(assegnazione password con le previste caratteristiche)
- 1.2 Obbligo di segretezza delle credenziali
- 1.3 Obbligo di diligente custodia delle credenziali con specifiche prescrizioni
- 1.4 Modifica trimestrale delle password dei dati sensibili
- 1.5 Disattivazione password non utilizzate per sei mesi
- 1.6 Antivirus aggiornato semestralmente
- 1.7 Obbligo di custodia di copie di sicurezza
- 1.8 Piano per il ripristino della disponibilità dei dati
- 1.9 Individuazione dei profili di autorizzazione
- 1.10 Revisione almeno annuale della conservazione dei profili di autorizzazione
- 1.11 Obbligo di impartire istruzioni per il salvataggio dei dati con frequenza almeno settimanale
- 1.12 Formazione del personale
- 1.13 Revisione annuale della lista degli incaricati
- 1.14 Aggiornamento annuale (semestrale per i dati sensibili) dei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggere i difetti
- 1.15 Protezione di strumenti elettronici e dati da trattamenti illeciti e da accessi non consentiti
- 1.16 Misure di sicurezza per il trattamento di dati personali affidato a soggetti esterni alle strutture
- 1.17 Misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi

### **2. MISURE IDONEE** (*Art. 31 D.Lgs. 196/2003*)

#### **2.1 MISURE ORGANIZZATIVE**

- 2.1.1 Istruzioni agli incaricati per assicurare la segretezza e la custodia delle password
- 2.1.2 Istruzioni in caso di assenza prolungata o impedimento dell'incaricato
- 2.1.3 Istruzioni per la custodia e l'uso dei supporti rimovibili al fine di evitare accessi non autorizzati
- 2.1.4 Istruzioni sui supporti rimovibili contenenti dati sensibili non utilizzati
- 2.1.5 Assegnazione codici per l'identificazione
- 2.1.6 Idonee procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e del sistema
- 2.1.7 Istruzioni per la custodia dei supporti e per l'installazione dei programmi operativi del sistema
- 2.1.8 Obbligo di non lasciare incustodito ed accessibile lo strumento elettronico
- 2.1.9 Redazione dei criteri per il ripristino dei dati in seguito a danneggiamento e distruzione
- 2.1.10 Descrizione dei criteri da adottare per garantire le misure minime in caso di trattamento affidato a soggetti esterni alla struttura
- 2.1.11 Redazione di appositi mansionari
- 2.1.12 Registrazione delle consultazioni
- 2.1.13 Altro (specificare) .....

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
**Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196**

---

**2.2 MISURE FISICHE**

- 2.2.1 Misure per garantire la protezione delle aree e dei locali rilevanti ai fini della custodia o della accessibilità
- 2.2.2 Vigilanza della sede
- 2.2.3 Ingresso controllato
- 2.2.4 Sistemi di allarme e/o sorveglianza
- 2.2.5 Registrazione degli accessi
- 2.2.6 Autenticazione degli accessi
- 2.2.7 Custodia in classificatori o armadi
- 2.2.8 Custodia in armadi blindati e/o ignifughi
- 2.2.9 Deposito in cassaforte
- 2.2.10 Custodia dei supporti in contenitori sigillati
- 2.2.11 Dispositivi antincendio
- 2.2.12 Continuità dell'alimentazione elettrica
- 2.2.13 Controllo sull'operato degli addetti
- 2.2.14 Verifica della leggibilità dei supporti
- 2.2.15 Altro (*specificare*) .....

**2.3 MISURE LOGICHE**

- 2.3.1 Registrazione degli accessi
- 2.3.2 Controlli aggiornati antivirus
- 2.3.3 Cifratura dei dati memorizzati
- 2.3.4 Cifratura dei dati trasmessi
- 2.3.5 Annotazione della fonte dei dati
- 2.3.6 Rilevazione delle intercettazioni
- 2.3.7 Verifiche periodiche per finalità
- 2.3.8 Verifiche automatizzate dei requisiti dati
- 2.3.9 Controllo su operato addetti alla manutenzione
- 2.3.10 Controllo supporti di manutenzione
- 2.3.11 Altro (*specificare*) .....

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
 Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196

**5.1 TABELLE**

**Tabella 1.1 - Elenco dei trattamenti: informazioni essenziali**

Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Altre Strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			
Trattamento di dati comunicati dall'odontoiatra ai fini della progettazione tecnica e fabbricazione del manufatto protesico/orteseo.	Pazienti dell'odontoiatra (soggetti per i quali si progetta e si crea il manufatto protesico/orteseo).	x		Laboratorio	Laboratori terzi per specifiche attività (se i dati non sono resi anonimi)	<input type="checkbox"/> Fax <input type="checkbox"/> Personal Computer <input type="checkbox"/> collegato/i <input type="checkbox"/> non collegato/i alla Rete Internet
Trattamento giuridico ed economico del personale e rilevazione delle presenze ai fini della tenuta dei libri obbligatori INAIL.	Personale dipendente e collaboratori.	x		Direzione/ Uff. Personale/ Uff. Amministrazione	CNA/Consulente del lavoro (che ha la possibilità di accedere all'applicativo e "modificare" le informazioni in esso contenute previa consultazione dell'impresa) che agisce come autonomo titolare/responsabile del trattamento	<input type="checkbox"/> Fax <input type="checkbox"/> Personal Computer <input type="checkbox"/> collegato/i <input type="checkbox"/> non collegato/i alla Rete Internet

**Tabella 1.2 - Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti <sup>1</sup>**

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
PA = dati riguardanti i pazienti	Data base contenente informazioni pazienti degli odontoiatri	<input type="checkbox"/> c/o Sede laboratorio <input type="checkbox"/> altro: _____	Personal computer	<input type="checkbox"/> Rete locale <input type="checkbox"/> Rete geografica <input type="checkbox"/> Rete Internet
D = dati riguardanti i dipendenti ed i collaboratori	Data base contenente informazioni riguardanti il personale dipendente ed i collaboratori	<input type="checkbox"/> c/o Sede laboratorio <input type="checkbox"/> altro: _____	Personal computer	<input type="checkbox"/> Rete locale <input type="checkbox"/> Rete geografica <input type="checkbox"/> Rete Internet

<sup>1</sup> Da compilare facoltativamente, collegandola alla tabella precedente, ad esempio attraverso l'identificativo

*Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti*

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Laboratorio	Elaborazione della scheda di progettazione tecnica e fabbricazione del manufatto protesico/orteseo	Acquisizione dei dati dei pazienti
Impiegata/o dell'Ufficio/Ufficio <input type="checkbox"/> personale <input type="checkbox"/> amministrativo <input type="checkbox"/> direzione	Rilevazione delle presenze dei dipendenti, raccolta dei giustificativi d'assenza, elaborazione prospetto paghe, anche ai fini della tenuta dei libri obbligatori INAIL (con il concorso di CNA/Consulente del lavoro), stampa su carta e consegna della "busta paga" per i dipendenti e del "compenso" per i collaboratori	Raccolta dei dati del personale mediante "rileva presenze", eventuale stampa e conservazione su supporto cartaceo del "libro presenze Inail", comunicazioni via e-mail/inserimento diretto su sito riservato alla struttura esterna che concorre al trattamento, consultazione di anagrafiche, elaborazione statistiche, utilizzo, ricezione dei dati elaborati tramite e-mail/tramite FTP dal sito riservato, stampa su carta e consegna della "busta paga" per i dipendenti e del "compenso" per i collaboratori

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
**Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196**

**Tabella 3 - Analisi dei rischi**

Rischi		Si / No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Comportamento degli operatori	sottrazione di credenziali di autenticazione		
	carenza di consapevolezza, disattenzione o incuria		
	comportamenti sleali o fraudolenti		
	errore materiale		
	altro evento		
Eventi relativi agli strumenti	azione di <i>virus</i> informatici o di programmi suscettibili di recare danno		
	<i>spamming</i> o tecniche di sabotaggio		
	malfunzionamento, indisponibilità o degrado degli strumenti		
	accessi esterni non autorizzati		
	intercettazione di informazioni in rete		
	altro evento		
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto		
	sottrazione di strumenti contenenti dati		
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria		
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)		
	errori umani nella gestione della sicurezza fisica		
	altro evento		

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
**Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196**

**Tabella 4.1 - Le misure di sicurezza adottate o da adottare**

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare (*)	Struttura o persone addette all'adozione
1. Antivirus aggiornati, divieto di installare software non testato.	Per evitare il danneggiamento sw e/o accesso non consentito, distruzione, perdita, modifica, invio di dati a terzi	Tutti (quelli relativi ai dipendenti e ai pazienti)	Aggiornamento antivirus obbligatorio quindicinale	Aggiornamento antivirus settimanale	
2. Gruppo di continuità, verifica all'impianto elettrico, verifica all'impianto di climatizzazione.	Danneggiamento hw e sw, distruzione, perdita di dati				
3. Continuo rinnovamento della tecnologia hardware e software.	Malfunzionamento, indisponibilità o degrado degli strumenti				
4. Sistemi di crittazione.	Accessi esterni non autorizzati				
5. Programmi antispamming.	Spamming o altre tecniche di sabotaggio				
6. Impianti d'allarme.	Asportazione e furto di strumenti contenenti dati				
7. Video-sorveglianza.	Asportazione e furto di strumenti contenenti dati				
8. Contratti con società di vigilanza.	Asportazione e furto di strumenti contenenti dati				

\* Indicare eventualmente i tempi previsti per l'adozione delle misure; attenzione a non indicare misure minime di sicurezza, che dovrebbero già essere presenti in azienda, come misure da adottare!!!

**Tabella 4.2 - Scheda descrittiva delle misure adottate <sup>2</sup>**

Scheda n.	_____	compilata da	_____	data di compilazione	_____
Misura					
Descrizione sintetica					
Elementi descrittivi					
Data aggiornamento					

<sup>2</sup> Da compilare facoltativamente

*Tabella 5.1 – Criteri e procedure per il ripristino della disponibilità dei dati*

Ripristino		
Banca/data base/archivio di dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
Data base contenente informazioni pazienti degli odontoiatri	Salvataggio su CD/altro supporto <input type="checkbox"/> giornaliero <input type="checkbox"/> settimanale tramite procedura automatizzata	
Data base contenete informazioni riguardanti il personale dipendente ed i collaboratori	Salvataggio su CD/altro supporto <input type="checkbox"/> giornaliero <input type="checkbox"/> settimanale tramite procedura automatizzata	

*Tabella 5.2 – Criteri e procedure per il salvataggio dei dati <sup>3</sup>*

Salvataggio			
Banca dati	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio
Data base contenente informazioni pazienti degli odontoiatri	Salvataggio su CD/altro supporto <input type="checkbox"/> giornaliero <input type="checkbox"/> settimanale tramite procedura automatizzata	Le copie sono conservate (in contenitore ignifugo) presso la sede aziendale <hr/> e presso <hr/>	
Data base contenete informazioni riguardanti il personale dipendente ed i collaboratori	Salvataggio su CD/altro supporto <input type="checkbox"/> giornaliero <input type="checkbox"/> settimanale tramite procedura automatizzata	Le copie sono conservate (in contenitore ignifugo) presso la sede aziendale <hr/> e presso <hr/>	

<sup>3</sup> Da compilare facoltativamente

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
**Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196**

**Tabella 6 – Pianificazione degli interventi formativi previsti**

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
<p>Intervento formativo rivolto al personale incaricato per renderlo edotto:</p> <ul style="list-style-type: none"> <li>• dei rischi che incombono sui dati,</li> <li>• delle misure disponibili per prevenire eventi dannosi,</li> <li>• dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività,</li> <li>• delle responsabilità che ne derivano;</li> <li>• delle modalità per aggiornarsi sulle misure minime adottate dal titolare,</li> </ul> <p>e costante aggiornamento attraverso materiale cartaceo</p>	<ul style="list-style-type: none"> <li>- Dipendenti dell'ufficio <ul style="list-style-type: none"> <li>□ personale,</li> <li>□ amministrativo,</li> <li>□ direzione,</li> </ul> </li> <li>- Incaricati operanti nel laboratorio</li> </ul>	<ul style="list-style-type: none"> <li>- Preventivamente al trattamento per tutti gli incaricati</li> <li>- al momento dell'ingresso in servizio nell'ipotesi di neo-assunti, stagisti, etc. ;</li> <li>- prima del trattamento nell'ipotesi di cambiamento di mansioni (incaricato) e nel caso di introduzione di nuovi elaboratori, programmi, sistemi informatici</li> </ul>

**Tabella 7 – Trattamenti affidati all'esterno**

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Elaborazione, salvataggio e ripristino delle informazioni riguardanti il personale dipendente ed i collaboratori.	Trattamento dei dati sensibili relativi al personale dipendente ed ai collaboratori necessari all'elaborazione del prospetto paghe	Cna/Consulente del lavoro (nominato responsabile/titolare del trattamento)	Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali

**Tabella 8 – Cifratura dei dati o separazione dei dati identificativi (solo per organismi sanitari ed esercenti professioni sanitarie)**

Trattamenti di dati	Protezione scelta (Cifratura/Separazione)	Tecnica adottata	
		Descrizione	Informazioni utili
Trattamento di dati comunicati dall'odontoiatra ai fini della progettazione tecnica e fabbricazione del manufatto protesico/orteseo			

**6. LETTERA DI COMUNICAZIONE DI ISTRUZIONI AGLI INCARICATI**

**[Intestazione impresa odontotecnica]**

Data,

Spett.le **nome e cognome**  
**dell'incaricato**

**Oggetto: Incarico ed istruzioni per il trattamento dei dati.**

L'incarico conferito comporta il trattamento di dati personali disciplinato dal Decreto Legislativo 30 giugno 2003, n. 196, la violazione delle cui norme è punita con sanzioni penali ed amministrative e con la responsabilità oggettiva per danno arrecato.

Le si impartiscono le istruzioni prodotte in allegato alla presente lettera di incarico, alle quali dovrà scrupolosamente e tassativamente attenersi.

Per l'accesso ai dati Le è fornita una parola chiave ed un codice identificativo personale.

Ai sensi, inoltre, di quanto previsto dall'allegato B del richiamato D.Lgs. n. 196/2003, in ragione della natura anche sensibile dei dati trattati sia con elaboratori che su supporto cartaceo, Lei viene espressamente autorizzato al trattamento dei relativi dati.

In particolare Le è richiesta la più scrupolosa osservanza delle informazioni e delle disposizioni che Le vengono impartite riguardanti la protezione degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta e degli interessi dell'impresa.

Sottoscrizione del titolare

.....

Sottoscrizione per presa visione e accettazione  
dell'incaricato: .....

**[N.B.: Allegare la sezione 6.1 di seguito riportata]**

**ALLEGATO** alla Lettera di comunicazione di istruzioni agli incaricati (punto 6)

**6.1 ISTRUZIONI AGLI INCARICATI**

Gli incaricati dei trattamenti di dati personali devono scrupolosamente attenersi alle seguenti istruzioni che devono essere considerate ordine di servizio.

a) Principi generali

I dati personali devono essere sempre trattati in modo lecito e secondo correttezza. Essi devono essere raccolti e registrati per scopi determinati, funzionali all'attività dell'azienda, espliciti e legittimi.

Tutto il personale è tenuto ad attivarsi per far sì che i dati trattati siano esatti e per quanto possibile aggiornati. I trattamenti non devono mai eccedere le finalità per le quali sono stati concepiti.

b) Definizioni

- Trattamento: sono quelle operazioni o complesso di operazioni, effettuate con o senza strumenti elettronici, concernenti raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, comunicazione, diffusione, cancellazione o distruzione di dati;
- Dato personale: è qualunque informazione relativa a persona fisica, giuridica, ente, impresa o associazione che ne consentano l'identificazione, diretta o indiretta;
- Dato sensibile: è il dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose o filosofiche, 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;
- Incaricato: il soggetto autorizzato dal titolare a compiere operazioni di trattamento dei dati.

c) Riservatezza dei dati personali

Il Personale deve sempre usare, all'interno come all'esterno dell'azienda, la massima discrezione sui dati personali di cui sia a conoscenza, curando attentamente la loro protezione.

Anche le comunicazioni tra colleghi di dati personali di terzi devono limitarsi a quanto necessario per l'espletamento delle proprie mansioni.

E' vietata ogni comunicazione di dati all'esterno dell'azienda, salvo il caso in cui ciò sia necessario per lo svolgimento degli incarichi affidati.

d) Utilizzo del materiale (computer e programmi)

Il Personale è tenuto ad utilizzare esclusivamente strumenti e programmi forniti o autorizzati dall'azienda, e soltanto per svolgere le mansioni d'ufficio. E' vietato l'utilizzo di floppy disc, di altri supporti o di programmi non autorizzati. I dispositivi (terminali e PC) devono essere disattivati durante le assenze (comprese le pause) dell'utente.

e) Utilizzo di password e username

Ad ogni dipendente è assegnata una o più coppie di username (identificativo utente) e password (parola chiave) personali, necessarie per accedere agli elaboratori e ai dati in essi contenuti. Il medesimo username non può, nemmeno in tempi diversi, essere assegnato a persone diverse.

**DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI**  
**Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196**

---

La password deve essere mantenuta segreta verso chiunque, compresi i colleghi di lavoro. A tale scopo è vietata l'evidenziazione o la memorizzazione della password con biglietti, messaggi e ogni altra modalità che ne comprometta la segretezza.

Ove si rendesse necessaria l'assegnazione di nuove password è fatto obbligo al personale di rivolgersi unicamente al titolare o al responsabile del trattamento.

L'utilizzo combinato di username e password attribuisce in modo univoco al loro titolare la responsabilità delle transazioni compiute.

La password può essere sostituita in ogni momento nel rispetto di quanto sopra. Deve essere sostituita entro le scadenze previste dalle procedure in uso per la disattivazione automatica, nonché quando vi sia anche il semplice sospetto che ne sia venuta meno la segretezza verso chiunque.

E' vietato l'utilizzo del medesimo username per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

La gestione delle password è riservata al preposto. In caso di dimenticanza, di anomalie o quando se ne dovesse ritenere l'opportunità, è sempre possibile richiederne il reset, con assegnazione di una nuova password iniziale.

f) Archivio e gestione dei documenti

Tutti i documenti cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi o degli armadi o contenitori in dotazione alle unità operative.

Massima attenzione dovrà essere posta per i documenti che si trovano in locali accessibili al pubblico.

L'accesso agli archivi è consentito al personale a ciò espressamente autorizzato in via permanente od occasionale.

Gli archivi devono essere mantenuti costantemente chiusi, compatibilmente con le esigenze di servizio.

Le copie dei documenti vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali.

Gli addetti ai servizi dove possono essere trattati dati sensibili o giudiziari dovranno porre massima attenzione al rispetto delle disposizioni precedenti.

Essi inoltre dovranno limitare al minimo indispensabile la giacenza della documentazione al di fuori degli armadi o contenitori muniti di serratura; controllare con particolare rigore l'accesso ai propri archivi; autorizzare e registrare eventuali accessi negli uffici compiuti al di fuori degli usuali orari di chiusura.

g) Accesso ai Computer

L'accesso ai terminali ed ai PC è consentito solo ai dipendenti dell'azienda; l'eventuale accesso di terzi è consentito solo se previamente autorizzato.

h) Sanzioni

L'inosservanza delle norme poste a tutela dei dati personali può determinare l'insorgere di responsabilità di tipo disciplinare, civile o anche penale, con l'applicazione – ove ne ricorrano i presupposti – delle relative sanzioni, oltre all'eventuale risarcimento del danno cagionato.

## 7. Piano per la formazione

**Attenzione:**

**i criteri devono essere individuati sulla base delle esigenze specifiche riscontrate in azienda**

*A titolo d'esempio:*

Il piano formativo del personale viene redatto tenendo conto dei seguenti criteri:

- a) aggiornamento annuale delle istruzioni agli incaricati
- b) verifica annuale delle istruzioni impartite agli incaricati
- c) aggiornamento sulle misure di sicurezza adottate
- d) .....

**8. Modulo di comunicazione della password**

Nome incaricato del trattamento .....

Password di accensione .....

Password di accesso alla rete.....

Area di appartenenza .....

Data .....

Firma dell'incaricato del trattamento

.....

**N.B.:**

**Questo modulo debitamente compilato deve essere riconsegnato in busta chiusa con, all'esterno, il nome dell'incaricato. Sarà cura dell'incaricato del trattamento comunicare immediatamente ogni variazione delle proprie password di accesso, utilizzando sempre il presente modulo e le medesime modalità.**

9. (Eventuale) Nota per controllo accesso di personale di pulizia di ditte esterne

[Intestazione Impresa odontotecnica]

Data, li .....

**Raccomandata a.r.**

Spett.le **Impresa Pulizie**

.....

**Oggetto: Misure di sicurezza ai sensi del D.Lgs. n. 196/2003.**

Come noto, con decorrenza 1° gennaio 2004 è entrato in vigore il D.Lgs. n.196/2003, recante il cosiddetto "Codice della Privacy" che, tra l'altro, prevede l'obbligo di adottare specifiche misure minime di sicurezza poste a tutela dei trattamenti dei dati personali.

**Tra i nuovi obblighi è previsto anche quello - in determinate circostanze - della "identificazione e registrazione dei soggetti ammessi agli archivi dopo l'orario di chiusura". Infatti, la protezione delle archiviazioni è estesa alla custodia e conservazione di ogni atto e documento cartaceo contenente dati personali particolari riferiti a soggetti fisici e giuridici.**

Allo scopo, in ottemperanza alle suddette necessità di legge, Vogliate cortesemente fornirci i nominativi delle persone che la Vostra ditta ha assegnato alle pulizie dei nostri locali di ....., e ciò anche al fine di poter considerare tali persone autorizzate all'accesso nei nostri locali.

In caso di assenza o impedimento delle persone che ci indicherete, sarà Vostra cura, ed obbligo, comunicarci i nominativi dei sostituti.

Ai fini dei controlli e delle responsabilità civili e penali connessi alla violazione delle norme contenute nel decreto sarà opportuno che la Vostra ditta organizzi un registro delle persone autorizzate ad accedere nei nostri locali. Le persone autorizzate dovranno limitarsi alle sole attività di pulizia. Il materiale cartaceo asportato destinato allo smaltimento dei rifiuti, dovrà essere riposto con cura negli appositi sacchi di plastica e, tali sacchi dovranno essere chiusi in maniera che gli atti e i documenti in essi contenuti non possano, nemmeno accidentalmente, fuoriuscire. Tale condotta dovrà essere rispettata dal Vostro personale che, allo scopo, sarà da Voi informato.

Distinti saluti.

Il Titolare

.....

**Indice**

<b>1. Scopo del documento</b>	pag. 2
<b>2. Organigramma della Sicurezza dei trattamenti</b>	pag. 2
<b>3. Inventario dei dispositivi, dei programmi e delle banche dati</b>	pag. 3
<b>4. Individuazione e valutazione dei rischi</b>	pag. 4
<b>5. Elenco delle misure di sicurezza</b>	pag. 5 – 6
<b>5.1 Tabelle</b>	pag. 7 - 12
<b>6. Lettera di comunicazione di istruzioni agli incaricati</b>	pag. 13
<b>6.1 Istruzioni agli incaricati (Allegato al punto 6)</b>	pag.14 - 15
<b>7. Piano per la formazione</b>	pag. 16
<b>8. Modulo di comunicazione della password</b>	pag. 17
<b>9. Nota per controllo accesso di personale di pulizia di ditte esterne</b>	pag. 18
<b>10. Indice</b>	pag. 19