

ASSOCIAZIONE ARTIGIANI
DELLA PROVINCIA DI VICENZA



Confartigianato



SPECIALE

Il nuovo Codice della Privacy

Seconda parte

**Schede riassuntive del Decreto Legislativo n. 196 del 30 giugno 2003
(Suppl. Ord. n. 123 alla G.U. 27.07.2003, n. 174)**

Continuiamo la pubblicazione della documentazione necessaria per l'applicazione del nuovo codice della Privacy. Nel precedente numero, sono state evidenziate le diversità tra la legge 675/96 e il Decreto Legislativo 196/03.

E' stata pure pubblicata una scheda di sintesi dei contenuti dell'ultimo Decreto Legislativo, con il fac simile del modello da utilizzare per l'informativa e per la raccolta del consenso rilasciato dal possessore dei dati.

Ricordiamo, come anticipato, che ogni impresa dovrà attuare, in ogni caso ed indipendentemente dal tipo di dato trattato (personale o sensibile) per la "salvaguardia" degli stessi, misure minime di sicurezza. Ciò vale sia nel caso di utilizzo di strumenti informatici che cartacei.

Ora riproduciamo due importanti documenti che dovranno essere utilizzati nel caso in cui l'impresa tratti dati definiti sensibili. Per la identificazione di questi si rimanda al precedente numero dello "Speciale Privacy" pubblicato nel numero del 9.04.04.

Il primo di questi è il fac simile del Documento programmatico per la sicurezza (DPS) che deve essere redatto nel caso in cui il trattamento dei dati sensibili avvenga a mezzo strumento informatico. Il DPS va attuato entro il 30 giugno p.v. o, entro il 1/1/2005 nel caso di obiettive ragioni tecniche che non consentano l'immediata applicazione delle misure minime di cui all'art. 34 del D.L. 196/03. Per la richiesta di proroga al 1 gennaio 2005, potrà essere utilizzato il modello riprodotto in questo "Specia-

le", inviandolo esclusivamente a mezzo posta elettronica (e-mail) al seguente indirizzo: www.garanteprivacy.it.

Il DPS, che dovrà essere rivisto con cadenza annua, ed entro il 31 marzo di ogni anno, non deve essere inviato presso nessun ente e nemmeno al Garante della Privacy. Andrà conservato presso l'impresa ed esibito in caso di richiesta da parte degli organi di verifica (Guardia di Finanza).

L'altro allegato, invece, sarà usato nel caso di trattamento di dati anche sensibili con supporti cartacei e contiene le misure minime da attuare in questa ipotesi.

Potrebbe essere la situazione che si viene a creare quando ad esempio una impresa che occupa personale dipendente affida la compilazione delle buste paga ad un terzo (Associazione, Consulente del lavoro). L'impresa "datore di lavoro", infatti, conosce i dati definiti sensibili dei propri dipendenti e che, di norma, non vengono trattati dalla stessa azienda per mezzo di mezzi informatici. In questo caso, il datore di lavoro dovrà fornire esatte istruzioni all'incaricato a compiere operazioni di trattamento del dato.

Anche questo documento, che dovrà essere aggiornato sempre entro il 31 marzo di ogni anno, verrà conservato all'interno dell'impresa ed esibito in caso di richiesta da parte degli organi verificatori. Nel caso invece che l'impresa con dipendenti provveda al proprio interno ad eseguire anche l'elaborazione delle paghe utilizzando procedure informatiche, dovrà attuare il DPS.

Intestazione Impresa

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

Pag. 1

**DOCUMENTO PER LA SICUREZZA
DEI TRATTAMENTI DI DATI PERSONALI**

Effettuati da:

Ragione sociale:

Indirizzo:

Sede operativa:

Partita IVA:

Attività:

Telefono:

Indice - sommario

1. Scopo del documento	pag. 2
2. Organigramma della Sicurezza dei trattamenti	pag. 2
3. Inventario dei dispositivi, dei programmi e delle banche dati	pag. 3
4. Individuazione e valutazione dei rischi	pag. 4
5. Elenco delle misure di sicurezza	pag. 5 - 6
6. Lettera di comunicazione di istruzioni agli incaricati	pag. 7
6.1 Istruzioni agli incaricati (Allegato al punto 6)	pag. 8 - 9
7. Piano per la formazione	pag. 10
8. Modulo di comunicazione della password	pag. 10
9. Nota per controllo accesso di personale di pulizia di ditte esterne	pag. 11

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

Pag. 2

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 intende garantire 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):

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

Pag. 3

. INVENTARIO DEI COMPUTER, DEI PROGRAMMI E DELLE BANCHE DATI (elettroniche e/o su carta)a) Identificazione e inventario dei computer

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

b) Identificazione, inventario ed analisi dei programmi aziendali

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

c) Identificazione, inventario ed analisi delle banche dati

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

d) Identificazione, inventario ed analisi dei supporti cartacei

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

e) Identificazione, inventario delle sedi nelle quali vengono effettuati i trattamenti

DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI

Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196

Pag. 4

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

<i>Risorsa</i>	<i>Fattore di rischio</i>	<i>R⁽¹⁾</i>	<i>Misura adottata⁽²⁾</i>
Risorse umane	1. Turn-over		
	2. Assenze		
	3. Ignoranza procedurale		
	4. ...		
Computer	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		
Programmi	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		
Dati	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		
Trasmissioni	35. Interruzione trasmissione		
	36. Malfunzionamento		
	37. Intercettazione volontaria		

⁽¹⁾ R deve essere espresso con la variabile di valutazione: **A = Alto; M = Medio; B = Basso**⁽²⁾ Individuare le misure, utilizzando l'unito elenco, riportando volta per volta la relativa numerazione.

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

Pag. 5

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
- 1.12 Revisione annuale della lista degli incaricati
- 1.13 Aggiornamento annuale (semestrale per i dati sensibili) dei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggere i difetti
- 1.14 Protezione di strumenti elettronici e dati per trattamenti illeciti e ad accessi non consentiti
- 1.15 Misure di sicurezza per il trattamento di dati personali affidato a soggetti esterni alle strutture
- 1.16 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

Pag. 6

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
Pag. 7

6. LETTERA DI COMUNICAZIONE DI ISTRUZIONI AGLI INCARICATI

[Intestazione ditta]

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]

DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI
Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196
Pag. 8

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

Pag. 9

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.

DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI

Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196

Pag. 10

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.

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

Pag. 11

9. (Eventuale) Nota per controllo accesso di personale di pulizia di ditte esterne**[Intestazione Impresa artigiana]**

Data, lì

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

.....

DOCUMENTO PER LA SICUREZZA DEI TRATTAMENTI DI DATI PERSONALI
Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196
Pag. 12

Nota Integrativa al D.P.S.

1. Descrizione delle misure adottate

Indicare brevemente in che cosa consistono ed eventualmente i criteri utilizzati.

Esempi:

Codice misura:

- 1.8 in cosa consiste il piano di ripristino della disponibilità dei dati
- 2.1.6 Individuare le procedure per la custodia di copie di sicurezza

2. Calendarizzazione delle verifiche, degli adempimenti e della formazione degli incaricati riferiti alle misure di sicurezza adottate

2.1 Registrazione delle verifiche trimestrali, semestrali, ed annuali

Indicare eventuali anomalie ed i conseguenti correttivi

2.2 Registrazione degli adempimenti con frequenza settimanale, trimestrale, semestrale ed annuale

Assicurare che siano stati effettuati

2.3 Registrazione semestrale od annuale degli interventi formativi degli incaricati

Indicare l'avvenuto aggiornamento delle istruzioni in precedenza impartite con riferimento alle misure di sicurezza contenute nel D.P.S.

Annotazione

Quanto riportato in questa scheda, costituisce il presupposto per l'aggiornamento o per la rielaborazione del D.P.S., la cui scadenza è fissata entro il 31 marzo di ogni anno.

Venerdì 16 aprile 2004

**LETTERA DI INCARICO E DI ISTRUZIONI AGLI INCARICATI PER IL
TRATTAMENTO DI DATI (ANCHE) SENSIBILI SU SUPPORTO CARTACEO**

[Intestazione ditta]

Data,

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

Oggetto: Incarico ed istruzioni per il trattamento dei dati su supporto cartaceo

Con riferimento all'intercorrente rapporto di lavoro Le viene conferito l'incarico concernente il trattamento dei dati personali, disciplinato dall'art. 35 del D.Lgs. n. 196/2003.

In ragione dell'incarico affidatoLe, uniamo le relative istruzioni alle quali dovrà attenersi con la dovuta diligenza e ciò per non incorrere nei provvedimenti previsti dalla normativa sopra richiamata, nonché dal C.C.N.L. di categoria.

Il titolare

.....

Sottoscrizione dell'incaricato
per presa visione e accettazione

.....

[N.B.: Allegare le istruzioni sotto riportate]

ALLEGATO alla Lettera di incarico**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

Si riportano, di seguito, alcune definizioni al fine di una migliore comprensione delle istruzioni impartite. Si intende per:

- **Trattamento**: quelle operazioni o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, il blocco, la comunicazione, la diffusione, la cancellazione o la distruzione di dati;
- **Incaricato**: il soggetto autorizzato dal titolare a compiere operazioni di trattamento dei dati;
- **Dato personale**: qualunque informazione relativa a una persona fisica, giuridica, ente, impresa o associazione che ne consentano l'identificazione, in via diretta o indiretta;
- **Dato sensibile**: 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;

Sono parificati ai dati sensibili i **dati giudiziari**, ossia i dati idonei a rivelare l'esistenza di procedimenti giudiziari, fallimentari o relativi al casellario giudiziale di una persona.

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) Archivio e gestione dei documenti

Il Personale è tenuto ad utilizzare esclusivamente strumenti forniti o autorizzati dall'azienda, e soltanto per svolgere le mansioni d'ufficio.

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, al fine di evitare rischi di distruzione o perdita degli stessi, di accesso non autorizzato, ovvero di trattamento non consentito o non conforme alle finalità di raccolta.

A tal fine, 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 e, comunque, non oltre il tempo necessario per l'esecuzione del servizio; 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 agli Archivi

L'accesso agli archivi 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.

Dichiarazione per usufruire della proroga al 1.01.2005

Ai sensi dell'art. 180 commi 2 e 3 del Codice sulla privacy, le misure di sicurezza possono essere adottate entro un anno dalla data di entrata in vigore del Codice stesso, qualora **obiettive ragioni tecniche** non consentano l'immediata applicazione delle misure minime di cui all'art. 34.

Il documento, **con data certa**, contenente le ragioni tecniche va conservato presso l'impresa, non mancando nel frattempo di adottare le misure di sicurezza possibili in relazione agli strumenti elettronici in proprio possesso, avendo tempo di adeguarli *al più tardi entro il 1 gennaio 2005*.

La dichiarazione potrebbe essere del seguente tenore:

«L'impresa _____ non ha potuto porre in essere tutte le misure di sicurezza prescritte dall'art. 34 del Decreto Legislativo 196/2003 in quanto queste richiedono un monitoraggio, oltre a quanto già in essere, relativamente al complesso sistema informatico aziendale / della struttura, nonché agli archivi cartacei; pertanto, le difficoltà tecniche ed organizzative, determinate dalla particolare struttura della scrivente, non consentono di rispettare il termine del 30 giugno 2004.

Ciò si certifica ai fini dell'applicazione di quanto previsto dall'art. 180 comma 3 del richiamato Decreto Legislativo.»