LAUDA Group S.r.l.
Via Raffaelle Sanzio, 7 - Cormano (MI)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Norma di riferimento D.l.g.196/03

1	22.06.2009	Revisione			
0	21.05.2004	I° Emissione			
N°	*Data*	*Descrizione*	***RGQ***	***RPD***	***DIR***
R E V I S I O N E			*Emesso*	*Verificato*	*Approvato*

Per ogni capitolo, di cui si compone la bozza del DPSS, si fa riferimento al paragrafo del manuale “Privacy: come cambiano le misure minime di sicurezza” che tratta dell’argomento, al fine di agevolare una rapida consultazione dei diversi argomenti, da parte dell’utilizzatore.

Indice

Documento programmatico sulla sicurezza	
1	L’elenco dei trattamenti dei dati personali
	1 Tipologie di dati trattati
	2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti
	3 La mappa dei trattamenti effettuati
2	Mansionario privacy ed interventi formativi degli incaricati
3	Analisi dei rischi che incombono sui dati
4	Misure atte a garantire l’integrità e la disponibilità dei dati
	1 La protezione di aree e locali
	2 La custodia e l’archiviazione di atti, documenti e supporti
	3 Le misure logiche di sicurezza
5	Criteri e modalità di ripristino dei dati
6	L’affidamento di dati personali all’esterno
7	Controllo generale sullo stato della sicurezza
8	Dichiarazioni d’impegno e firma
	Scheda analitica descrittiva dei singoli trattamenti
	Scheda analitica descrittiva delle singole misure di sicurezza
	Allegato A) – Tabella di supporto al paragrafo 1.1
	Allegato B) – Guida operativa per redigere il DPSS pubblicata dal Garante in data 11 giugno 2004
Documento per beneficiare del più lungo termine del 31.12.2004 per adeguarsi	
1	La descrizione degli strumenti tecnicamente inadeguati
2	Le ragioni dell’inadeguatezza tecnica
3	Gli interventi previsti per procedere all’adeguamento
4	I tempi dell’adeguamento
5	Le spese previste
6	Dichiarazione finale di impegno

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, LETTERA G) DEL DLGS 196/2003, E DEL DISCIPLINARE TECNICO ALLEGATO AL MEDESIMO DECRETO SUB B)
(Riferimenti: ottavo capitolo, paragrafi 8.1 e 8.2 del manuale)

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato da *Cognome e nome o denominazione del Titolare*……*con sede in*……..……*Codice fiscale*……(nel seguito del documento indicato come Titolare).

==========

Se il documento è redatto da un responsabile per la sicurezza, aggiungere:
Il presente documento è redatto e firmato in calce dal responsabile per la sicurezza, i cui dati sono i seguenti:

- *Nome e Cognome……., Qualifica all'interno dell'organizzazione……., nominato con lettera del……*(se persona fisica interna all'organizzazione*)*

oppure

- *Cognome e nome o denominazione del Responsabile……., con sede in……., rappresentato da……., nominato con lettera / contratto del……*(se responsabile esterno*)*.

==========

Conformemente a quanto prescrive il punto 19. del Disciplinare tecnico, allegato sub b) al Dlgs 196/2003, nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare), mediante:
   - la individuazione dei tipi di dati personali trattati
   - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
   - la elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati (analisi del mansionario privacy, punto 19.2 del disciplinare) e previsione di interventi formativi degli incaricati del trattamento (punto 19.6 del disciplinare)
3. l'analisi dei rischi che incombono sui dati (punto 19.3 del disciplinare)
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati (punto 19.4 del disciplinare)
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento (punto 19.5 del disciplinare)
6. i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno (punto 19.7 del disciplinare)
7. le procedure da seguire per il controllo sullo stato della sicurezza
8. dichiarazioni d'impegno e firma.

Indice

1	L'elenco dei trattamenti dei dati personali	Pag.
	1 Tipologie di dati trattati	
	2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti	
	3 La mappa dei trattamenti effettuati	
2	Mansionario privacy ed interventi formativi degli incaricati	Pag.
3	Analisi dei rischi che incombono sui dati	Pag.
4	Misure atte a garantire l'integrità e la disponibilità dei dati	Pag.
	1 La protezione di aree e locali	
	2 La custodia e l'archiviazione di atti, documenti e supporti	
	3 Le misure logiche di sicurezza	
5	Criteri e modalità di ripristino dei dati	Pag.
6	L'affidamento di dati personali all'esterno	Pag.
7	Controllo generale sullo stato della sicurezza	Pag.
8	Dichiarazioni d'impegno e firma	Pag.
Allegati		
	(Facoltativo) Schede analitiche descrittive dei singoli trattamenti	
	(Facoltativo) Schede analitiche descrittive delle singole misure di sicurezza	

1. L'elenco dei trattamenti dei dati personali

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, si procede come segue:

- si individuano i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili, distinguendo nell'ambito di questi ultimi quelli idonei a rivelare lo stato di salute e la vita sessuale, nonché quelli idonei a rivelare l'affezione da virus HIV e quelli di natura genetica) ed alla categoria di soggetti cui essi si riferiscono (clienti, fornitori, utenti, pazienti, personale…..)
- si descrivono le aree, i locali e gli strumenti con i quali si effettuano i trattamenti
- si elabora la mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti.

1.1 Tipologie di dati trattati

(Riferimenti: terzo capitolo, paragrafo 3.1 del manuale)

La bozza diffusa dal Garante precisa che "in questa sezione sono individuati i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne".

I dati trattati dal Titolare si possono suddividere come segue:

1 - Dati comuni relativi a clienti / utenti / consumatori
2 - Dati comuni relativi a fornitori
3 - Dati comuni relativi ad altri soggetti
4 - Dati biometrici relativi a clienti / personale / …….
5 - Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone ed oggetti
6 - Dati relativi allo svolgimento di attività economiche ed alle informazioni commerciali
7 - Dati di natura giudiziaria relativi a …….
8 - Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile
9 - Dati di natura anche sensibile relativi a clienti / utenti / membri / pazienti…….
10 Dati idonei a rivelare lo stato di salute e/o la vita sessuale di pazienti / degenti……
11 - Dati idonei a rivelare l'affezione da virus HIV
12 - Dati di natura genetica

***Nota bene**: l'elenco sopra esposto è puramente esemplificativo. Nei casi concreti, esso deve essere compilato in base alle tipologie ed alle banche di dati gestite dal Titolare. In ogni caso, si deve porre un accento particolare sulla eventuale presenza, nell'ambito di una categoria di dati trattati, di dati di natura sensibile o giudiziari.*

***Tabelle di supporto**: Per la individuazione dei dati che vengono trattati, ci si può avvalere di quanto è prestampato nell'allegato c) – elenco delle categorie di dati oggetto del trattamento al vecchio modello di notifica al Garante, combinato con quanto illustrato nelle istruzioni del nuovo modello di notifica, in vigore dal 1° gennaio 2004.*

In tale contesto, la puntuale indicazione delle tipologie di dati trattati si ottiene combinando le seguenti coordinate:

- ***tipi** di dati trattati*
- ***categorie di soggetti** cui tali dati si riferiscono.*

*Nell'Allegato **A – Tabella di supporto al paragrafo 1.1**, che è in calce alla presente Bozza, è contenuto un elenco di entrambe le coordinate, ottenuto dalla elaborazione dei modelli di notifica al Garante.*

1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

(Riferimenti: terzo capitolo, paragrafi 3.2 e 3.2.1 del manuale)

Il trattamento dei dati personali avviene nei **seguenti edifici**:

Palazzina degli uffici

E' situata in …….., in zona centrale / semiperiferica / periferica / industriale. All'interno di tale palazzina, esiste una **area ad accesso controllato**, alla quale si può accedere dopo avere passato il controllo di uno strumento, che procede al riconoscimento dell'iride.

Stabilimento

E' situato in…….., in zona industriale.

==========

Il trattamento dei dati personali avviene con i **seguenti strumenti**:

A – Schedari ed altri supporti cartacei

I supporti cartacei, ivi inclusi quelli contenenti immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, come segue:

- Archivio 1, localizzato nella palazzina degli uffici, in cui si raccolgono le pratiche e gli schedari relativi ai clienti professionali, di natura comune, ed in generale i dati di natura comune
- Archivio 2, localizzato nell'Ufficio Personale, nel quale si raccolgono le pratiche e gli schedari relativi ai dipendenti, anche di natura sensibile
- Archivio 3, localizzato nell'area ad accesso controllato della palazzina, in cui si raccolgono le pratiche e gli schedari contenenti dati di natura sensibile, che si riferiscono a soggetti diversi dal personale
- Archivio 4, localizzato nello stabilimento, in cui si raccolgono le pratiche e gli schedari relativi ai rapporti con i fornitori, di natura comune.
- ……..

B – Elaboratori non in rete

Per elaboratori non in rete si intendono quelli non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici.

Essi sono costituiti da:

- numero ….postazioni fisse, dislocate come segue:
  - …..nella palazzina uffici, nell'area che non è ad accesso controllato
  - …..nell'area ad accesso controllato della palazzina uffici
  - …..nello stabilimento
- numero…….computer portatili, dati in dotazione a……..

C – Elaboratori in rete privata

Per elaboratori in rete privata si intendono quelli accessibili, da altri elaboratori o più in generale da altri strumenti elettronici, solo attraverso reti proprietarie, sulle quali possono viaggiare unicamente i dati del titolare del sistema.

Si dispone di una rete, realizzata mediante collegamenti interni via cavo, costituita da:

- numero ….server, localizzati nell'area ad accesso controllato della palazzina uffici
- numero……postazioni, dislocate come segue:
  - …..nella palazzina uffici, nell'area che non è ad accesso controllato
  - …..nell'area ad accesso controllato della palazzina uffici
- numero…..stampanti, di cui …..sono dislocate nell'area ad accesso controllato
- numero…….altri strumenti elettronici (scanner, dispositivo di backup…..), dislocati prevalentemente nell'area ad accesso controllato.

D – Elaboratori in rete pubblica

Per elaboratori in rete pubblica si intendono quelli che utilizzano, anche solo per alcuni tratti, reti di telecomunicazione disponibili al pubblico, ivi inclusa la rete Internet.

Si dispone di una rete pubblica costituita da:

- numero……..server, localizzati nella palazzina degli uffici
- numero…..postazioni, dislocate come segue:
  - …..nella palazzina uffici, nell'area che non è ad accesso controllato
  - …..nell'area ad accesso controllato della palazzina uffici
  - …..nello stabilimento
- numero ……stampanti, di cui ……dislocate nella palazzina uffici e ……nello stabilimento
- numero…….altri strumenti elettronici (modem, router, scanner, dispositivi di backup…..), dislocati prevalentemente negli uffici.

I seguenti PC, pur non essendo fisicamente in rete con altri, dispongono di collegamento ad Internet:

- numero……fissi, dislocati come segue:
  - …..nella palazzina uffici, nell'area che non è ad accesso controllato
  - …..nell'area ad accesso controllato della palazzina uffici
  - …..nello stabilimento
- numero……portatili, assegnati al personale con funzioni commerciali.

E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti

Sono installati tre impianti di videosorveglianza:

- il primo, atto a proteggere le aree dai tentativi di intrusione, si compone di ……..apparecchi, dislocati intorno al perimetro sia della palazzina uffici, che dello stabilimento
- il secondo, atto a tutelare la sicurezza dei lavoratori, è installato nel reparto……dello stabilimento
- il terzo, atto a monitorare le condizioni di salute dei pazienti, è installato…….

F – Altri strumenti (es. basati su dati biometrici, patologie, dati genetici……)

Uno strumento, basato sul riconoscimento dell'iride delle persone, è installato nella zona che permette l'accesso ad un'area della palazzina: tale area è quindi ad accesso controllato.

1.3 La mappa dei trattamenti effettuati

(Riferimenti: terzo capitolo, paragrafo 3.3 del manuale)

Incrociando le coordinate di cui ai due paragrafi precedenti, si ottiene la mappa dei trattamenti di dati personali effettuati dal Titolare.

In relazione al diverso grado di rischio, è opportuno distinguere i trattamenti che vengono posti in essere nelle tre distinte aree in cui sono dislocati gli strumenti, nei casi in cui la circostanza è significativa (per gli schedari e gli elaboratori non in rete).

Il simbolo **0**, apposto nella casella di incrocio, significa che determinati tipi di dati sono trattati con determinati strumenti:

*In alternativa, invece del simbolo **0** potrebbe essere opportuno inserire uno specifico **identificativo di ciascun trattamento**, come suggerisce la bozza proposta dal Garante: "l'Identificativo del trattamento consiste in un codice, facoltativo, ma utile per il titolare, in quanto consente un'identificazione univoca e più rapida di ciascun trattamento, nella compilazione delle tabelle". Se si opta per questa soluzione, la frase diviene la seguente:*

Nelle caselle di incrocio si appone un simbolo, identificativo di ciascun trattamento, che sta tra l'altro a significare che determinati tipi di dati sono trattati con determinati strumenti.

TIPI DI DATI TRATTATI

1 - Dati comuni relativi a clienti / utenti / consumatori	A1	A2		A4	A5		A7	A8	A9		
2 - Dati comuni relativi a fornitori	B1	B2		B4	B5		B7	B8	B9		
3 - Dati comuni relativi ad altri soggetti		C2			C5		C7	C8	C9		
4 - Dati biometrici relativi a clienti / personale / …….		D2			D5			D8	D9		D11
5 - Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone / oggetti		E2			E5			E8	E9	E10	
6 - Dati relativi allo svolgimento di attività economiche e a informazioni commerciali		F2			F5		F7	F8	F9		
7 - Dati di natura giudiziaria relativi a …….		G2			G5			G8	G9		
8 - Dati relativi al personale, nonché a candidati per diventarlo, anche sensibili		H2			H5			H8	H9		
9 - Dati di natura anche sensibile relativi a clienti / utenti / membri / pazienti…….			I3			I6		I8	I9		
10 Dati idonei a rivelare lo stato di salute e/o la vita sessuale di pazienti / degenti……			K3			K6		K8			
11 - Dati idonei a rivelare l'affezione da virus HIV			L3			L6		L8			
12 - Dati di natura genetica			M3			M6					
	As	**Au**	**Ac**	**Bs**	**Bu**	**Bc**	**Bp**	**C**	**D**	**E**	**F**

STRUMENTI UTILIZZATI

Legenda degli strumenti utilizzati per il trattamento:

A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:
- **As** quelli custoditi nello stabilimento
- **Au** quelli custoditi nell'area ad accesso non controllato della palazzina uffici
- **Ac** quelli custoditi nell'area ad accesso controllato della palazzina uffici

B – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:
- **Bs** quelli localizzati nello stabilimento
- **Bu** quelli localizzati nell'area ad accesso non controllato della palazzina uffici
- **Bc** quelli localizzati nell'area ad accesso controllato della palazzina uffici
- **Bp** quelli portatili

C – Elaboratori in rete privata

D – Elaboratori in rete pubblica

E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti

F – Altri strumenti (es. basati su dati biometrici).

***Nota**: qualora si ritenesse opportuno allegare al DPSS le eventuali "Schede analitiche dei singoli trattamenti", il cui modello – elaborato in base alla bozza proposta dal Garante – è in calce al presente lavoro, il simbolo identificativo del trattamento coinciderebbe con quello indicato nella tabella sopra esposta (per cui, ad esempio, l'identificativo A1-A2-A4-A5-A7-A8-A9 si riferirebbe alla scheda analitica predisposta per i trattamenti di dati comuni relativi a clienti / utenti / fornitori).*

Da una prima lettura della mappa, si possono apprezzare gli accorgimenti adottati per ridurre i rischi:
- i dati di natura genetica (12) vengono trattati esclusivamente nell'area ad accesso controllato, con strumenti diversi da quelli elettronici o con computer non in rete, ivi localizzati
- i dati idonei a rivelare l'affezione da virus HIV (11) vengono trattati esclusivamente nella palazzina uffici, nell'ambito della quale sono archiviati nell'area ad accesso controllato e trattati con strumenti elettronici diversi da quelli in rete pubblica. I server della rete privata sono inoltre localizzati nell'area ad accesso controllato della palazzina uffici
- in generale, i dati sensibili e giudiziari non vengono trattati, né archiviati, nello stabilimento, e non sono inoltre presenti nei computer portatili affidati in dotazione a…….

2. Mansionario privacy ed interventi formativi degli incaricati

(Riferimenti: secondo capitolo, paragrafi 2.2, 2.2.1, 2.2.2 e 2.2.3 del manuale)

Per il trattamento dei dati personali, il Titolare:

- **non ha nominato responsabili**

oppure

- **ha nominato i seguenti responsabili**, attribuendo loro incarichi di ordine organizzativo e direttivo, come segue *(scegliere uno o più dei punti di cui sotto e, eventualmente, aggiungere):*
  - responsabile per la sicurezza, il cui compito è di progettare, realizzare e mantenere in efficienza le misure di sicurezza, conformemente a quanto previsto dagli articoli 31 e 33 Dlgs 196/2003, nella persona di……..(*ovvero* nella persona esterna / società esterna…….)
  - amministratore del sistema informativo, cui è conferito il compito di sovrintendere alle risorse del sistema informativo e di consentirne l'utilizzazione, nella persona di……(*ovvero* nella persona esterna / società esterna…….)
  - responsabile per garantire il soddisfacimento dei diritti esercitabili dai soggetti interessati, ai sensi degli articoli da 7 a 10 Dlgs 196/2003, nella persona di…….
  - un responsabile per i trattamenti effettuati da ogni funzione aziendale, il cui elenco è presente nel Sito della rete di comunicazione http://www.XXXX.it (*in alternativa*, il cui elenco è reso conoscibile mediante…….)
  - un responsabile per i trattamenti effettuati da ogni divisione aziendale, il cui elenco è presente nel Sito della rete di comunicazione http://www.XXXX.it (*in alternativa*, il cui elenco è reso conoscibile mediante…….)
  - un responsabile per i trattamenti effettuati da ogni filiale, il cui elenco è presente nel Sito della rete di comunicazione http://www.XXXX.it (*in alternativa*, il cui elenco è reso conoscibile mediante…….)
  - un responsabile per i trattamenti effettuati da ogni punto di vendita, il cui elenco è presente nel Sito della rete di comunicazione http://www.XXXX.it (*in alternativa*, il cui elenco è reso conoscibile mediante…….).

==========

(Riferimenti: secondo capitolo, paragrafi 2.3, 2.3.1, 2.3.2, 2.3.3, 2.3.4 e 2.3.5 del manuale)

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante (*scegliere tra 1., 2. e 3.*):

1. designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito
2. documentata preposizione di ogni persona ad una unità, per la quale sia stato previamente individuato per iscritto l'ambito del trattamento, consentito agli addetti all'unità medesima
3. documentata preposizione di ogni persona ad una unità, per la quale sia stato previamente individuato per iscritto l'ambito del trattamento, consentito agli addetti all'unità medesima o, in taluni casi, designazione per iscritto di un singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
- procedure per il salvataggio dei dati
- modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

==========

(Riferimenti: secondo capitolo, paragrafo 2.4 del manuale)
Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (**mansionario privacy**), nell'ambito del trattamento dei dati personali.
Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.
La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

Nella seguente matrice si riassumono i tratti salienti dell'attuale mansionario privacy, come segue:

- sull'asse verticale si riportano i dati personali oggetto di trattamento, quali emergono dall'analisi effettuata nel paragrafo 1. del presente documento
- sull'asse orizzontale si riportano le unità organizzative ("**strutture di riferimento"**) in cui si suddivide l'organizzazione del Titolare
- l'apposizione del simbolo **0**, in corrispondenza della casella di intersezione tra le due coordinate, significa che una determinata unità organizzativa procede al trattamento dei dati indicati nelle righe:

TIPI DI DATI TRATTATI

1 - Dati comuni relativi a clienti / utenti / consumatori		0		0	0			0	0			
2 - Dati comuni relativi a fornitori			0									
3 - Dati comuni relativi ad altri soggetti				0								
4 - Dati biometrici relativi a clienti / personale / …….	0	0										
5 - Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone / oggetti	0					0		0	0			
6 - Dati relativi allo svolgimento di attività economiche e alle informazioni commerciali				0				0	0			
7 - Dati di natura giudiziaria relativi a …….	0											
8 - Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile	0											
9 - Dati di natura anche sensibile relativi a clienti / utenti / membri / pazienti…….		0		0		0						
10 Dati idonei a rivelare lo stato di salute e/o la vita sessuale di pazienti / degenti……						0	0					
11 - Dati idonei a rivelare l'affezione da virus HIV						0	0					
12 - Dati di natura genetica							0					
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**L**	**M**	**N**

UNITA' ORGANIZZATIVE

La legenda delle unità organizzative ("**strutture di riferimento"**) è la seguente:
A – Ufficio personale
B – Contabilità clienti
C – Contabilità fornitori
D – Ufficio commerciale
E – Ufficio acquisti
F – Staff medico
G – Ufficio R & S
H – Singole filiali, aventi analoghi compiti
I – Singoli punti di vendita, aventi analoghi compiti
L - …….....
M - …….....
N - …….....

La bozza proposta dal Garante viene precisato che il termine ***Struttura di riferimento*** *indica "la struttura (ufficio, funzione, ecc…) all'interno della quale viene effettuato il trattamento. In caso di strutture complesse, è possibile indicare la macro – struttura (direzione, dipartimento o servizio del personale) oppure gli uffici specifici all'interno della stessa (ufficio contratti, sviluppo risorse, controversie sindacali, amministrazione – contabilità).*
La bozza del Garante suggerisce di descrivere sinteticamente l'organizzazione di ogni struttura, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati. Si possono utilizzare anche specifici riferimenti a documenti già predisposti (provvedimenti, ordini di servizio, regolamenti interni, circolari), indicando le precise modalità per reperirli.
Nella prima versione della bozza, il Garante riteneva che come fosse opportuno indicare anche il ***responsabile della struttura****, cioè il ruolo o la qualifica del dirigente o del responsabile della struttura (in questa sede, al termine responsabile si deve attribuire un significato gerarchico, non di responsabile del trattamento ai sensi della normativa privacy). In sede di redazione della bozza finale, le richiesta di tale informazione non è più presente.*
Ulteriori informazioni che, alla luce di quanto suggerisce la bozza del Garante, può essere opportuno fornire sono le seguenti:

- ***trattamenti operati dalla struttura****, descrivendo i trattamenti per i quali ciascuna struttura ha primaria responsabilità. Ad esempio, si potrà osservare che per i dati della categoria "1.- Dati comuni relativi a clienti / utenti / consumatori" la primaria responsabilità è dell'unità organizzativa D – Ufficio commerciale, mentre per le altre unità (B, E, H, I) il trattamento è limitato a talune fasi, strettamente necessarie per lo svolgimento dei propri compiti*
- ***compiti di ogni struttura****, descrivendo sinteticamente i compiti e le responsabilità della struttura, in ciascuno dei trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica operativa della base dati (salvataggi, ripristini, eccetera). Anche in questo caso è possibile utilizzare altri documenti (provvedimenti, ordini di servizio, regolamenti interni, circolari) già predisposti, indicando le precise modalità per reperirli.*

==========

(Riferimenti: sesto capitolo, paragrafo 6.5.2 del manuale)
Sono previsti **interventi formativi degli incaricati del trattamento**, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per la sicurezza o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

(*Facoltativo*) In ogni caso, sono previste riunioni periodiche, in numero di …..l'anno, per fare il punto sull'evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali.

(*Facoltativo*) Per l'anno 2004, è previsto che, mediamente, ogni incaricato dedichi …giornate lavorative alla formazione in materia di trattamento dei dati personali.

(Facoltativo, tratto dalla bozza predisposta dal Garante) Nella seguente tabella si riassume un quadro sintetico dell'impegno formativo che si prevede di sostenere, nell'anno 2004, in attuazione della normativa privacy:

	CORSO 1	CORSO 2	CORSO n
Corso di formazione / intervento formativo			
Descrizione sintetica			
Classi di incarico interessate			
Numero di incaricati interessati *(facoltativo)*			
Numero di incaricati già formati / da formare nell'anno (*facoltativo*)			
Tempi previsti			
Spesa prevista (*facoltativo*)			

Legenda della tabella:

- ***corso di formazione**: riporta l'identificativo del corso di formazione*
- ***descrizione sintetica**: descrivere sinteticamente gli obiettivi e le modalità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 (ingresso in servizio o cambiamento di mansioni degli incaricati, introduzione di nuovi elaboratori, programmi o sistemi 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, anche in riferimento alle strutture di appartenenza*
- ***tempi previsti:** indicare i tempi previsti per lo svolgimento degli interventi formativi*
- ***numero di incaricati interessati**: contiene il numero di addetti interessati al corso. L'indicazione di tale dato, presente nella bozza originaria del DPSS, non è più prevista, nel documento finale pubblicato dal Garante*
- ***numero di incaricati già formati / da formare nel corso dell'anno**: contiene l'indicazione del numero di addetti già formati negli anni precedenti e quelli di cui si prevede la formazione nell'anno in corso. L'indicazione di tale dato, presente nella bozza originaria del DPSS, non è più prevista, nel documento finale pubblicato dal Garante*
- ***spesa prevista:** tale dato non è presente, nella bozza del DPSS pubblicata dal Garante.*

3. Analisi dei rischi che incombono sui dati

(Riferimenti: quarto capitolo, paragrafo 4.1 del manuale)

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono
- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

==========

Nella seguente matrice si procede a una stima del grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

	ELVATISSIMO				**12** Dati di natura genetica
GRADO DI INTERESSE PER I TERZI	**ALTO**	**1** Dati comuni clienti utenti consumatori	**6** Dati svolgimento di attività economiche		**11** Dati affezione da virus HIV
	MEDIO	**3** Dati comuni altri soggetti		**9** Dati sensibili clienti utenti membri pazienti	**10** Dati stato di salute e/o vita sessuale
	BASSO	**2** Dati comuni di fornitori	**4** Dati biometrici clienti personale **5** Dati idonei a rilevare la posizione	**7** Dati di natura giudiziari a **8** Dati sensibili personale	
		BASSO	**MEDIO**	**ALTO**	**ELEVATISSIMO**

PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO

Si nota che un grado di rischio alto, o addirittura elevatissimo, è collegato al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- quelli idonei a rivelare informazioni di carattere sensibile o giudiziario dei soggetti interessati, che sono accomunati dall'aspetto critico di avere un elevato grado di pericolosità per la privacy dei soggetti interessati
- quelli che costituiscono una importante risorsa, commerciale e tecnologica, per il Titolare, in relazione ai danni che conseguirebbero da una eventuale perdita, o trafugamento, dei dati.

==========

Per quanto concerne gli **strumenti impiegati per il trattamento**, le componenti di rischio possono essere idealmente suddivise in:

1. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
   - al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti)
   - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici)
2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti)
3. rischio di penetrazione logica nelle reti di comunicazione
4. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti.

*La bozza proposta dal Garante contiene il seguente **elenco degli eventi**, che possono generare danni e che comportano rischi per la sicurezza dei dati personali. Il documento stesso precisa che tale elenco deve considerarsi una lista esemplificativa, da prendere in considerazione come base di partenza:*

Comportamento degli operatori
- sottrazione di credenziali di autenticazione
- carenza di consapevolezza, disattenzione o incuria
- comportamenti sleali o fraudolenti
- errore materiale
Eventi relativi agli strumenti
- azione di virus informatici o di programmi suscettibili di recare danno
- 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
- ingressi non autorizzati a locali / aree ad accesso ristretto
- sottrazione di strumenti contenenti dati
- eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali…), nonché dolosi, accidentali o dovuti a incuria
- guasto a sistemi complementari (impianto elettrico, climatizzazione…)
- errori umani nella gestione della sicurezza fisica

La bozza precisa che "è possibile, per ulteriori dettagli, rinviare a documenti analoghi già redatti in tema di piani di sicurezza e gestione del rischio, come AD ESEMPIO Business Continuità Plan, Disaster Recovery Plan, ecc…(tenendo però presente che le analisi alla base di questi altri documenti possono avere una natura ben diversa).

Nella seguente tabella si evidenziano i fattori di rischio cui sono soggetti gli strumenti con cui l'organizzazione procede al trattamento dei dati personali. Il simbolo **o**, posto nella casella di intersezione, significa che l'esposizione al rischio è modesta; il simbolo **O** significa che l'esposizione al rischio è elevata

TIPI DI DATI TRATTATI

Rischio d'area, legato al verificarsi di eventi distruttivi	O	O	O	O	O	O	O	O	O	O	O
Rischio d'area, legato all'accesso non autorizzato nei locali	O	O	o	O	O	o	O	o	O	O	O
Rischio di guasti tecnici di hardware, software e supporti				O	O	O	O	o	o	o	o
Rischio di penetrazione logica nelle reti di comunicazione									O		
Rischio legato ad atti di sabotaggio e ad errori umani	o	o	o	o	o	o	o	O	O	o	o
	As	**Au**	**Ac**	**Bs**	**Bu**	**Bc**	**Bp**	**C**	**D**	**E**	**F**

STRUMENTI UTILIZZATI

Legenda degli strumenti utilizzati per il trattamento:
A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:
- **As** quelli custoditi nello stabilimento
- **Au** quelli custoditi nell'area ad accesso non controllato della palazzina uffici
- **Ac** quelli custoditi nell'area ad accesso controllato della palazzina uffici

B – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:
- **Bs** quelli localizzati nello stabilimento
- **Bu** quelli localizzati nell'area ad accesso non controllato della palazzina uffici
- **Bc** quelli localizzati nell'area ad accesso controllato della palazzina uffici
- **Bp** quelli portatili

C – Elaboratori in rete privata
D – Elaboratori in rete pubblica
E – Impianti di videosorveglianza ed altri idonei a rilevare immagini, suoni e posizione di persone ed oggetti
F – Altri strumenti (es. basati su dati biometrici).

Nell'elaborare la tabella, si è tenuto conto anche di alcuni fattori legati alla struttura del Titolare, nei seguenti termini:
- il rischio d'area, legato alla eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento, è giudicato inferiore per l'area ad accesso controllato, all'interno della palazzina, rispetto a quanto accade per gli altri luoghi in cui si svolge l'attività, con conseguente diminuzione del rischio:
  - per gli archivi esistenti in tale area
  - per gli elaboratori in rete privata, in relazione al fatto che i server sono ubicati in tale area
  - per i personal computer non in rete, localizzati in tale area
- il rischio di guasti tecnici delle apparecchiature interessa i soli strumenti elettronici: in tale contesto, è giudicata più rischiosa la situazione degli strumenti non in rete che, essendo affidati a singoli che non sempre possiedono un bagaglio tecnico adeguato, presentano un rischio di rottura maggiore, rispetto agli impianti che vengono gestiti da persone con specifiche competenze, quali quelli in rete, quello di sorveglianza e quello per la rilevazione di dati biometrici
- il rischio di penetrazione logica nelle reti di comunicazione interessa, essenzialmente, i soli strumenti che sono tra loro collegati tramite una rete di comunicazione accessibile al pubblico
- il rischio legato ad atti di sabotaggio, o ad errori umani delle persone, presente in tutte le tipologie di strumenti utilizzati, è maggiore per quelli che sono in rete.

La bozza del Garante suggerisce, su base facoltativa, di predisporre una tabella riassuntiva, in cui si commenta quale possa essere l'impatto sulla sicurezza dei dati, in relazione a ciascun evento, e valutare la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'evento (anche in termini sintetici: es. alta / media / bassa). In questo modo è possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare.

Data di compilazione (*facoltativa*): ……..

Rischi	SI/NO	Descrizione dell'impatto sulla sicurezza (gravità: alta / media / bassa)
Comportamenti 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 *virus* informatici o di programmi suscettibili di recare danno		
Spamming 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, ...)		
Errori umani nella gestione della sicurezza fisica		
Altro evento		

Il Garante precisa infine che "l'analisi dei rischi può essere condotta utilizzando metodi di complessità diversa: l'approccio descritto nella bozza del DPSS predisposta dall'Autorità è volto solo a consentire una prima riflessione in contesti che, per dimensioni ridotte o per altre analoghe ragioni, non ritengano di dovere procedere ad una analisi più strutturata". Letta a contrario, tale affermazione conferma che, nella maggior parte dei casi, l'analisi dei rischi non deve essere condotta come se si fosse la CIA, ma si risolve più semplicemente in una presa di coscienza, e nella conseguente formalizzazione nel DPSS, dei diversi rischi cui sono soggetti i trattamenti di dati personali.

4. Misure atte a garantire l'integrità e la disponibilità dei dati

Nel presente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede alla descrizione:

- delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata, anche per adeguarsi alle novità introdotte dal Dlgs 196/2003, e dal disciplinare tecnico in materia di misure minime di sicurezza, allegato a tale decreto sub b).

*Qualora fossero state predisposte, su base facoltativa, le **schede analitiche dei singoli trattamenti** e le **schede analitiche descrittive delle singole misure di sicurezza**, anche utilizzando i modelli che si ottengono dalla elaborazione del DPSS proposto dal Garante (si veda in calce alla presente bozza), si può fare riferimento a tale circostanza, con una frase del seguente tenore:*

Al presente Documento programmatico sulla sicurezza vengono inoltre allegate le Schede analitiche dei singoli trattamenti e/o le Schede analitiche descrittive delle singole misure di sicurezza, che costituiscono parte integrante del Documento programmatico sulla sicurezza stesso.

4.1 La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da (*riportare i dispositivi di cui si è dotati, nessuno dei quali è esplicitamente imposto dalla normativa sulle misure minime di sicurezza*):

- dispositivi antincendio *(da considerare obbligatori ai sensi del Dlgs 626/94 e successive modifiche, NdR)*
- gruppo di continuità dell'alimentazione elettrica
- impianto di condizionamento
- ……

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da (*riportare i dispositivi di cui si è dotati, nessuno dei quali è esplicitamente imposto dalla normativa sulle misure minime di sicurezza*):

- sistemi di registrazione ed autenticazione degli accessi negli uffici
- sistemi di allarme e/o di sorveglianza antintrusione
- vigilanza da parte di personale interno (*o* di una ditta specializzata), anche durante l'orario di apertura (*o* nelle ore di chiusura)
- accesso controllato alle aree in cui si svolgono i trattamenti più critici, mediante:
  - sistemi di rilevazione delle caratteristiche biometriche
  - tesserino magnetico
  - ……

  Tale regola è tassativa per i dati relativi all'identità genetica, in relazione al fatto che la norma prescrive che essi possono essere trattati esclusivamente all'interno di locali protetti, accessibili ai soli incaricati dei trattamenti ed ai soggetti specificamente autorizzati ad accedervi.
- ……..

==========

Gli impianti ed i sistemi di cui è dotata l'organizzazione:

- appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per l'anno 2004 sono quindi previsti semplicemente interventi di manutenzione

oppure

- saranno oggetto di importanti interventi, nel corso del 2004, al fine di migliorare ulteriormente le misure di sicurezza delle strutture, nelle quali si svolge il trattamento dei dati personali. In particolare, si prevede di effettuare i seguenti investimenti:

Descrizione dell'investimento	Spesa preventivata

4.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, dischetti, fotografie, pellicole….), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

==========

(Riferimenti: quinto capitolo, paragrafo 5.1 del manuale)

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento, o direttamente al titolare.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

==========

(Riferimenti: quinto capitolo, paragrafo 5.2 del manuale)
Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.
Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli incaricati sono stati dotati di (*scegliere uno o più*):

- cassetti con serratura
- armadi chiudibili a chiave
- cassaforte
- …….

nei quali devono riporre i documenti, contenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.
Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Particolari cautele vengono previste per il trasporto di documenti, atti e supporti contenenti di relativi all'identità genetica, all'esterno dei locali riservati al loro trattamento: per questi casi, è stato prescritto che il trasporto debba avvenire in contenitori muniti di serratura, o utilizzando dispositivi equipollenti.

==========

(Riferimenti: quinto capitolo, paragrafo 5.2 del manuale)
Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa deve avvenire in luoghi , armadi , casseforti, o dispositivi equipollenti, che possono essere chiusi.

Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione dei seguenti accorgimenti (*indicare uno o più*):

- sono dotati di strumenti elettronici per il controllo degli accessi (ad esempio, tesserino magnetico distribuito agli incaricati autorizzati)
- ad alcune persone, aventi la scrivania prospiciente, viene dato l'incarico di vigilare gli archivi, dettando precise istruzioni in merito al fatto che una persona deve essere sempre presente, durante l'orario di apertura dell'archivio, per controllare chi vi accede
- alcuni dipendenti svolgono la mansione di addetti all'archivio
- le persone vengono autorizzate preventivamente ad accedere agli archivi, previa richiesta della chiave all'incaricato che ha il compito di custodirla
- ……

Si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, mediante l'adozione dei seguenti accorgimenti (*indicare uno o più)*:

- gli archivi sono dotati di strumenti elettronici per il controllo degli accessi, che mantengono in memoria le informazioni su chi abbia avuto accesso ed in quale lasso di tempo
- la chiave dell'archivio è affidata, dopo l'orario di chiusura, al titolare o ai responsabili del trattamento, o in alternativa ad uno o più soggetti incaricati per iscritto, i quali provvedono ad annotare in un apposito registro i nominativi di cloro che hanno richiesto di accedere all'archivio
- ……

==========

Gli impianti e le attrezzature, di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari:

- appaiono soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti. Per l'anno 2004, sono quindi previsti semplicemente interventi di manutenzione e di rimpiazzo

oppure

- saranno oggetto di importanti interventi, nel corso del 2004, al fine di migliorare ulteriormente l'efficacia delle misure di custodia ed archiviazione dei dati. In particolare, si prevede di effettuare i seguenti investimenti:

Descrizione dell'investimento	Spesa preventivata
Miglioramento della sicurezza delle aree di archiviazione	
Dotazione delle aree di archiviazione di nuovi strumenti e dispositivi	
Acquisto di cassetti chiudibili a chiave	
Acquisto di armadi e casseforti chiudibili a chiave	
……	

4.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato
- realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative
- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus)
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD….), nei quali siano contenuti dati personali.

==========

(Riferimenti: sesto capitolo, paragrafo 6.1 del manuale)

Il **sistema di autenticazione informatica** viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente con strumenti elettronici non contenenti dati personali, o contenenti solo dati personali destinati alla diffusione.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle **credenziali di autenticazione** per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si utilizzano i seguenti metodi (*scegliere uno o più*):

- si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente
- si attribuisce un dispositivo di autenticazione (tesserino magnetico, smart card…….) all'incaricato, prescrivendo che il suo possesso ed uso devono avvenire esclusivamente da parte dell'incaricato stesso
- si associa l'attribuzione di un dispositivo di autenticazione, posseduto ed utilizzato esclusivamente dell'incaricato, ad un codice identificativo o ad una parola chiave
- si è dotati di dispositivi che rilevano una caratteristica biometrica degli incaricati (fisica, quale l'impronta digitale, la forma della mano, l'iride, la retina, o comportamentale, quale la firma o la voce)
- si associa un dispositivo, che rileva una caratteristica biometrica dell'incaricato, ad un codice identificativo o ad una parola chiave.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.
  Se la struttura attuale del Titolare non permette di agire, per il momento, in tale senso, aggiungere:
  Tale regola diverrà tassativa, allorché il Titolare avrà completato il processo di adeguamento a quanto prescritto dal Dlgs 196/2003, entro il 30 giugno 2004 (*in alternativa, si può scrivere* "entro il 31 dicembre 2004" *se il Titolare, in relazione al fatto di possedere mezzi elettronici tecnicamente inadeguati, redige entro il 30/6/2004 un documento avente data certa, per avvalersi di tale più lungo termine*).
  Sino ad allora, saranno presenti alcuni casi in cui la medesima credenziale di autenticazione è attribuita a due o più persone, limitatamente alle seguenti ipotesi:
  - per l'accesso, da parte degli incaricati, ad elaboratori non in rete, le cui caratteristiche non consentono l'autonoma sostituzione delle parole chiave
  - per l'accesso, da parte degli amministratori del sistema informativo, ad elaboratori in rete, il cui sistema operativo prevede un unico livello di accesso per tale funzione
- nei casi in cui una componente della credenziale di autenticazione è costituita dal codice per l'identificazione (username), attribuito all'incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.
  Se la struttura attuale del Titolare non permette di agire, per il momento, in tale senso, aggiungere:
  Tale regola diverrà tassativa, allorché l'organizzazione avrà completato il processo di adeguamento a quanto prescritto dal Dlgs 196/2003, entro il 30 giugno 2004 (*in alternativa, si può scrivere* "entro il 31 dicembre 2004" *se il Titolare, in relazione al fatto di possedere mezzi elettronici tecnicamente inadeguati, redige entro il 30/6/2004 un documento avente data certa, per avvalersi di tale più lungo termine*).
  Sino ad allora, limitatamente agli elaboratori che non sono in rete, saranno presenti alcuni casi in cui uno stesso codice di identificazione è assegnato a due o più incaricati.
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Se la struttura attuale del Titolare non permette di agire, per il momento, in tale senso, aggiungere:
Tali regole diverranno tassative, allorché l'organizzazione avrà completato il processo di adeguamento a quanto prescritto dal Dlgs 196/2003, entro il 30 giugno 2004 (*in alternativa, si può scrivere* "entro il 31 dicembre 2004" *se il Titolare, in relazione al fatto di possedere mezzi elettronici tecnicamente inadeguati, redige entro il 30/6/2004 un documento avente data certa, per avvalersi di tale più lungo termine*).
Sino ad allora, limitatamente agli elaboratori che non sono in rete, saranno presenti alcuni casi in cui le credenziali di autenticazione non verranno disattivate, qualora ciò non fosse di fatto possibile (ad esempio, perché la medesima credenziale è stata attribuita a due o più incaricati, alcuni dei quali mantengono la qualità per accedere all'elaboratore).

Agli **incaricati vengono impartite precise istruzioni** in merito ai seguenti punti:

- dovere di custodire i dispositivi, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici (ad esempio, il tesserino magnetico o la smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici (viene prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo come se fosse una carta di credito). In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza all'amministratore di sistema, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:

- immediatamente, non appena viene consegnata loro da chi amministra il sistema
- successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, pippobaudo….)
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata
- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

==========

(Riferimenti: sesto capitolo, paragrafo 6.2 del manuale)

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, si osserva che:

- non appare necessario prevedere profili di autorizzazione distinti, per le diverse persone, in relazione alle limitate dimensioni della struttura del Titolare ed al fatto che non si ravvisano ragioni di tutela della riservatezza tali, da imporre che uno o più incaricati non possano accedere ad alcune tipologie di dati personali oggetto di trattamento (*ipotesi applicabile in casi in cui le dimensioni siano veramente limitate, come può ad esempio accadere per uno studio professionale, o una piccola impresa, nella quale le poche persone che utilizzano gli strumenti elettronici hanno titolo per accedere a tutte le tipologie di dati personali trattati con gli elaboratori)*

oppure

- si è impostato un sistema di autorizzazione, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative. L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

  Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.

  Il profilo di autorizzazione non viene in genere studiato per ogni singolo incaricato, ma è generalmente impostato per classi omogenee di incaricati (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale). L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato o di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

  Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

==========

(Riferimenti: sesto capitolo, paragrafi 6.3.1, 6.3.2, 6.5.3 e 6.6 del manuale)
Per quanto riguarda la **protezione, di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).
A tale fine, si è dotati di idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento, di regola:

- ogni……giorni / mesi nel caso di strumenti elettronici in rete pubblica
- ogni……giorni / mesi nel caso di strumenti elettronici in rete privata
- ogni……giorni / mesi nel caso di strumenti elettronici che non sono in rete.
  Se il Titolare non prevede che, per il momento, gli strumenti che non sono in rete siano dotati di programmi antivirus, aggiungere:
  Per quanto riguarda questi ultimi, la loro dotazione di strumenti e programmi antivirus verrà completata entro il 30 giugno 2004 (*in alternativa, si può scrivere* "entro il 31 dicembre 2004" *se il Titolare, in relazione al fatto di possedere mezzi elettronici tecnicamente inadeguati, redige entro il 30/6/2004 un documento avente data certa, per avvalersi di tale più lungo termine*).

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, che il nuovo codice privacy ha reso obbligatoria per i casi in cui si trattino dati sensibili o giudiziari.
A tale riguardo (*scegliere una delle formule sottostanti*):

1. la nostra organizzazione si è da tempo dotata di tali strumenti, per la protezione degli elaboratori in rete
2. la nostra organizzazione non necessita di tali strumenti, in quanto non tratta dati sensibili o giudiziari con elaboratori in rete
3. la nostra organizzazione si doterà di tali strumenti entro il 30 giugno 2004 (*in alternativa, si può scrivere* "entro il 31 dicembre 2004" *nel caso in cui il Titolare, in relazione al fatto di possedere mezzi elettronici tecnicamente inadeguati, redige entro il 30/6/2004 un documento avente data certa, per avvalersi di tale più lungo termine*).

(Obbligatorio per gli organismi sanitari e per gli esercenti le professioni sanitarie)
Per il trattamento di dati idonei a rivelare lo stato di salute o la vita sessuale, si adottano particolari accorgimenti, con il fine di:

- rendere temporaneamente inintelligibili tali dati, anche a chi è autorizzato ad accedervi: per l'accesso a tali dati, gli incaricati autorizzati devono compiere una particolare azione (ad esempio, inserire una ulteriore parola chiave), in mancanza della quale l'accesso ai dati è impedito
- garantire loro una particolare protezione, con l'utilizzo di tecniche crittografiche al fine di cifrare il contenuto dei file, in modo che il loro contenuto possa essere letto solo da incaricati in possesso di un particolare codice
- permettere la identificazione degli interessati solo in caso di necessità.

Un particolare accorgimento viene previsto per il trasferimento di dati di natura genetica, prevedendo che esso debba avvenire in modo cifrato, mediante l'utilizzo della crittografia: a tale fine si è adottato il sistema della firma digitale, basata su una infrastruttura tecnologica di crittografia a chiave pubblica.

Il terzo aspetto riguarda l'utilizzo di appositi programmi, la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici, tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete, e di correggere di conseguenza i difetti insiti negli strumenti stessi. A tale riguardo (*scegliere una delle formule sottostanti*):

1. la nostra organizzazione si è da tempo dotata di tali programmi, per la protezione da malfunzionamenti degli strumenti elettronici, che provvede ad aggiornare con cadenza almeno annuale, che diviene semestrale per gli strumenti con i quali si trattano dati sensibili o giudiziari
2. la nostra organizzazione si doterà di tali programmi entro il 30 giugno 2004 (*in alternativa, si può scrivere* "entro il 31 dicembre 2004" *se il Titolare, in relazione al fatto di possedere mezzi elettronici tecnicamente inadeguati, redige entro il 30/6/2004 un documento avente data certa, per avvalersi di tale più lungo termine*). Successivamente, l'aggiornamento di tali programmi avverrà con cadenza almeno annuale, che diviene semestrale per gli strumenti con i quali si trattano dati sensibili o giudiziari.

==========

(Riferimenti: sesto capitolo, paragrafo 6.4 del manuale)

Per quanto concerne i **supporti rimovibili** (es. floppy disk, dischi ZIP, CD….), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

==========

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici:

- appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati. Per l'anno 2004, sono quindi previsti semplicemente interventi finalizzati all'aggiornamento, alla manutenzione ed a qualche rimpiazzo

oppure

- saranno oggetto di importanti interventi, nel corso del 2004, al fine di migliorare ulteriormente l'efficacia di tali misure. In particolare, si prevede di effettuare investimenti per le finalità indicate nella seguente tabella:

Descrizione dell'investimento	Spesa preventivata
Realizzare / migliorare il sistema di autenticazione informatica	
a) apparecchi e strumenti	
b) programmi	
c) formazione specifica	
Realizzare / migliorare il sistema di autorizzazione	
a) apparecchi e strumenti	
b) programmi	
c) formazione specifica	
Realizzare / migliorare il sistema di protezione	
a) apparecchi e strumenti	
b) programmi	
c) formazione specifica	

5. Criteri e modalità di ripristino dei dati

(Riferimenti: sesto capitolo, paragrafo 6.4 del manuale)

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

==========

(Facoltativo) I documenti cartacei, e gli eventuali supporti diversi da quelli elettronici, contenenti dati personali, vengono fotocopiati / scannerizzati / microfilmati con cadenza…….. I supporti contenenti le copie vengono:

- trasferiti in luoghi diversi dalla sede aziendale, quali *descrivere*

e/o

- archiviati in armadi ignifughi / casseforti / ……, qualora le dimensioni del supporto lo permettano (es. CD).

==========

(*Facoltativo*) Per i trattamenti effettuati con strumenti elettronici, durante l'orario di lavoro, il Titolare dispone di sistemi RAID (Redundant array of inexpensive disks): si tratta di hard disk multipli, visti però dal sistema operativo come un singolo disco, che garantiscono la disponibilità e l'integrità dei dati, anche nel caso di guasto hardware di uno dei dischi che compongono il sistema.

==========

Per i dati trattati con strumenti elettronici, sono previste procedure di backup, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni (CD, dischi ZIP…..).

Il salvataggio dei dati trattati avviene come segue:

- la frequenza è giornaliera / ogni due giorni / ……../ settimanale (*la norma impone una frequenza almeno settimanale)*
- si utilizzano supporti differenti, da quelli in cui sono contenuti i dati dei salvataggi eseguiti la volta precedente
- per ciascun salvataggio, si eseguono……..copie *(la norma non impone di eseguire più di una copia*).

Le copie vengono custodite:

- in luoghi protetti della sede (ad esempio, in una cassaforte ignifuga dislocata nell'area ad accesso controllato)

e/o

- in luoghi diversi dalla sede (ad esempio, vengono portate a casa dal responsabile per la sicurezza o, in sua assenza, da una delle due persone all'uopo designate. Durante il trasporto vengono custodite in valigetta munita di serratura e, nell'abitazione del depositario, vengono depositate in una cassaforte).

(Facoltativo) La struttura operativa, o la persona, incaricati di effettuare il salvataggio e di controllarne l'esito è……

==========

(Facoltativo) Per fronteggiare gli eventi con impatto catastrofico, è costituito un centro di back-up, realizzato (*scegliere*):

- predisponendo una struttura del tipo scatola vuota (di proprietà dell'organizzazione, o di tipo consortile o "in service")
- raddoppiando il centro ed integrandolo in rete
- creando un centro di recovery (che può essere di proprietà dell'organizzazione, o di tipo consortile o "in service")
- ……

==========

(Facoltativo) E' previsto un piano di continuità operativa, che ha lo scopo di garantire la continuità e la disponibilità, degli strumenti e dei dati, in ipotesi di danneggiamenti causati da eventi accidentali, sabotaggi, disastri naturali: l'obiettivo di tale piano è di ripristinare i servizi informatici entro…….giorni e di rendere minime le perdite causate dall'interruzione dell'attività.

==========

(Facoltativo) Periodicamente, con cadenza almeno mensile / trimestrale / semestrale vengono effettuate, a cura della persona / struttura incaricata del salvataggio, delle prove di ripristino, mediante l'esecuzione di appositi test di efficacia delle procedure di salvataggio e di ripristino dei dati adottate.

==========

(Facoltativo) Gli investimenti programmati per il 2004, finalizzati a garantire il ripristino dei dati in termini ragionevoli, sono i seguenti:

Descrizione dell'investimento	Spesa preventivata
Riproduzione dei dati contenuti in atti e documenti cartacei	
Realizzazione di sistemi RAID	
Investimenti in strumenti di backup	
Realizzazione di un centro di backup	
Realizzazione e mantenimento di un piano di continuità operativa	
……..	

6. L'affidamento di dati personali all'esterno

(Riferimenti: settimo capitolo del manuale)

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

In ogni caso, il soggetto cui le attività sono affidate dichiara:

1. di essere consapevole che i dati che tratterà, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione della normativa per la protezione dei dati personali
2. di ottemperare agli obblighi previsti dalla normativa per la protezione dei dati personali
3. di attenersi alle istruzioni specifiche, eventualmente ricevute per il trattamento dei dati personali, conformando ad esse anche le procedure eventualmente già in essere
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate, e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Qualora il trasferimento dovesse avvenire verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano (*scegliere uno dei seguenti punti*):

- rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico
- consegni una copia del documento programmatico sulla sicurezza redatto, ovvero consegni una copia del certificato di conformità rilasciato da chi ha curato la progettazione e l'attuazione delle misure minime di sicurezza, nel caso in cui il destinatario abbia affidato a soggetti esterni tali compiti.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.
(*Facoltativo*) Allo stato attuale, risultano nominati come responsabili:

- la persona / associazione / ente / società……per i trattamenti di dati……..al fine di……..
- la persona / associazione / ente / società……per i trattamenti di dati……..al fine di……..

(Facoltativo, dalla bozza suggerita dal Garante) Allo stato attuale, il quadro sintetico delle attività trasferite a terzi, che comportano il trattamento di dati personali, è il seguente:

	ATTIVITA' 1	ATTIVITA' 2	ATTIVITA' n
Descrizione sintetica dell'attività esternalizzata			
Trattamenti di dati interessati			
Soggetto esterno delegato			
Descrizione dei criteri e degli impegni assunti per l'adozione delle misure			
Data delle verifiche *(facoltativa)*			

Legenda:

- ***descrizione dell'attività esternalizzata****: indicare sinteticamente l'attività affidata all'esterno*
- ***trattamenti di dati interessati****: indicare i trattamenti di dati, ponendo un particolare accento sulla eventualità che essi siano sensibili o giudiziari, effettuati nell'ambito dell'attività esternalizzata*
- ***soggetto esterno delegato****: indicare la società, l'ente o il consulente cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento)*
- ***descrizione dei criteri e degli impegni assunti per garantire l'adozione delle misure****: perché sia garantito un adeguato trattamento dei dati, è necessario che il soggetto a cui è affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale*
- ***data delle verifiche:*** *contiene l'indicazione del numero e delle date indicative delle verifiche eventualmente previste. L'indicazione di tale dato, presente nella prima bozza del DPSS proposta dal Garante, è stata omessa nella versione definitiva.*

7. Controllo generale sullo stato della sicurezza

(Riferimenti: sesto capitolo, paragrafo 6.3.1.2 del manuale)

Al responsabile per la sicurezza è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.
(*Esempio*) A tale fine, è previsto che:

- al responsabile venga affidato un budget annuo di euro…….., che può utilizzare in autonomia, a condizione che il singolo investimento non superi l'importo di euro……
- per singoli investimenti, che superino l'importo di euro……., il responsabile dovrà ottenere l'autorizzazione di……
- ogni……mesi è prevista una riunione del responsabile per la sicurezza con i membri del Consiglio di Amministrazione, durante la quale il responsabile renderà conto delle somme spese e, se la situazione lo richiede, si provvederà eventualmente ad aumentare il budget annuo di spese.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile per la sicurezza e le persone da questo appositamente incaricate provvedono con frequenza settimanale / mensile, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento

- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette
- verificare l'integrità dei dati e delle loro copie di backup
- verificare la sicurezza delle trasmissioni in rete
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti
- verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.
Dell'attività di verifica svolta viene redatto un verbale, che viene conservato dal Titolare (*eventualmente*: e allegato al Documento programmatico sulla sicurezza).

(*Facoltativo*) Periodicamente, con frequenza…….(generalmente annuale, ma a volte semestrale, o addirittura trimestrale per le organizzazioni più complesse), ci si rivolge ad una società specializzata, che effettua l'audit di sicurezza: con tale termine si intende l'attività di verifica, che potrà avvenire in modo estemporaneo, anche con verifiche casuali e non annunciate.
Obiettivo dell'audit di sicurezza è di verificare che tutte le misure implementate, sia quelle tecnologiche che quelle organizzative, svolgano correttamente le funzionalità per cui sono state adottate.

8. Dichiarazioni d'impegno e firma

(Riferimenti: ottavo capitolo, paragrafo 8.2 del manuale)
Il presente documento, redatto nel …….20XX, viene firmato in calce da:
- ……., in qualità di rappresentante legale del Titolare
- *(eventuale)*……., in qualità di responsabile per la sicurezza.

(Facoltativo) Ad esso si allegano, quale parte integrante del Documento programmatico sulla sicurezza stesso:
- n….schede analitiche descrittive dei singoli trattamenti
- n….schede analitiche descrittive delle singole misure di sicurezza.

(Nei casi in cui è previsto che il documento debba essere oggetto di approvazione, da parte di organi del Titolare)
Il presente Documento programmatico sulla sicurezza verrà sottoposto per l'approvazione al Consiglio di Amministrazione (*o organo, anche unipersonale, avente funzioni analoghe*), e successivamente trascritto nel libro sociale che riporta le delibere prese dallo stesso.

L'originale del presente documento viene custodito presso la sede della società, per essere esibito in caso di controlli.
Una sua copia verrà consegnata (*scegliere uno o più*):
- a ciascun responsabile interno del trattamento dei dati personali
- ai responsabili esterni del trattamento dei dati personali
- a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali (ad esempio, nel caso in cui dovessimo essere nominati responsabili per determinati trattamenti di dati personali).

(Per i soggetti tenuti a redigere la relazione sulla gestione, da allegare al bilancio di esercizio)
Nella relazione accompagnatoria del bilancio di esercizio si riferisce dell'avvenuta redazione del presente documento, che costituisce (*scegliere*):
- la prima redazione del Documento programmatico sulla sicurezza
- l'aggiornamento annuale del Documento programmatico sulla sicurezza, originariamente redatto in data……..

Luogo e data……..
Firma del rappresentante legale del Titolare……
(Eventualmente) Firma del responsabile per la sicurezza……

SCHEDA ANALITICA DESCRITTIVA DEI SINGOLI TRATTAMENTI

Nella presente scheda, che è stata elaborata sulla base di quanto suggerisce il Garante, si riportano le informazioni analitiche in merito alle caratteristiche dei trattamenti, che la organizzazione del Titolare pone in essere, ed alle misure di sicurezza che si devono di conseguenza adottare.
A titolo indicativo, si deve compilare una scheda analitica per ogni tipologia di trattamenti posta in essere, avendo riguardo, ai fini della individuazione di quali siano le distinte tipologie, ai tipi di dati trattati ed alle categorie di soggetti cui tali dati si riferiscono: ad esempio, nel caso esposto nel paragrafo 1.1 della presente bozza del DPSS è opportuno predisporre una scheda analitica per ognuno dei dodici trattamenti indicati.
Il Garante precisa che "le informazioni possono essere completate o sostituite da schemi, tabelle, disegni di architettura del sistema informativo o da altri documenti aziendali già compilati e idonei a fornire in altro modo le informazioni medesime".

Data di compilazione……(la data di compilazione della scheda è particolarmente utile, nei casi in cui essa sia compilata in data significativamente diversa (antecedente) rispetto alla redazione finale del DPSS).

Prima Sezione - Informazioni essenziali sul trattamento (in questa sezione sono individuati i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura - ufficio, funzione, ecc…- interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati. Nella redazione della lista si può tenere conto anche delle informazioni contenute nelle notificazioni eventualmente inviate al Garante anche in passato).

CAMPO	SPIEGAZIONE FORNITA DAL GARANTE
Identificativo del trattamento *(facoltativo)*	Consiste in un codice, facoltativo, ma utile per il titolare, in quanto consente l'identificazione univoca e più rapida di ciascun trattamento. Nel presente lavoro, il codice identificativo è quello attribuito nel paragrafo 1.3: ad esempio, la scheda che si riferisce a 1. Dati comuni relativi a clienti / utenti / consumatori riporterà l'identificativo "A1+A2+A4+A5+A7+A8+A9".
Descrizione sintetica del trattamento	Menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita e dell'attività svolta (es. fornitura di beni o servizi, gestione del personale, ecc…) e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc…).
Natura dei dati trattati	Dovrà essere posto un particolare accento sulla presenza, o meno, di dati sensibili o giudiziari.
Struttura di riferimento	Indicare la struttura (ufficio, funzione, eccetera), all'interno della quale viene effettuato il trattamento. In caso di strutture complesse, è possibile indicare la macro-struttura (es. direzione, dipartimento o servizio del personale), oppure gli uffici specifici all'interno della stessa (es. ufficio contratti, ufficio paghe, sviluppo risorse, ufficio controversie sindacali, amministrazione – contabilità, eccetera).
Altre strutture (anche esterne) e funzioni che concorrono al trattamento	Nel caso in cui un trattamento, per essere completato, comporti l'attività di diverse strutture è opportuno indicare, oltre a quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento, anche dall'esterno.
Eventuale banca dati *(facoltativo)*	Indicare eventualmente la banca dati (ovvero il data base o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i dati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati: in tale caso elencare le diverse banche dati.
Luogo di custodia dei supporti di memorizzazione *(facoltativo)*	Indicare il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano (in quale sede, centrale o periferica, o presso quale fornitore di servizi, eccetera) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, eccetera) ed ogni altro supporto rimovibile. Il punto può essere approfondito meglio in occasione di aggiornamenti.
Descrizione degli strumenti e dei dispositivi di accesso utilizzati per il trattamento	Elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: - supporti cartacei - altri supporti diversi dagli elaboratori elettronici - strumenti elettronici (elaboratori o PC anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi; terminale non intelligente, palmare, telefonino eccetera).
Tipologia di	Descrizione sintetica e qualitativa della rete informatica che collega i

interconnessione *(facoltativo)*	dispositivi di accesso utilizzati dagli incaricati ai dati: elaboratori non in rete, rete locale o privata, rete pubblica, Extranet, Internet, eccetera.
Seconda Sezione - Misure di sicurezza in essere o da adottare (in questa sezione devono essere riportate, in forma sintetica, le misure in essere e da adottare a contrasto dei rischi, individuati dall'analisi dei rischi. Per misura si intende non solo lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia. Le misure da adottare possono essere inserite in una sezione dedicata ai programmi per migliorare la sicurezza).	
CAMPO	SPIEGAZIONE FORNITA DAL GARANTE
Misure di sicurezza	Descrizione sintetica delle misure di sicurezza adottate, per il trattamento in esame (seguendo anche le indicazioni contenute nelle altre regole dell'Allegato B del Codice privacy)
Rischio contrastato	Per ciascuna misura indicare sinteticamente i rischi che si intende contrastare (seguendo anche le indicazioni contenute nelle altre regole dell'Allegato B del Codice privacy) .
Trattamenti interessati	Indicare i trattamenti interessati per ciascuna delle misure adottate. Determinate misure possono non essere riconducibili a specifici trattamenti o banche di dati (ad esempio, con riferimento alle misure per la protezione delle aree e dei locali).
Data di effettività	Per ogni misura è necessario indicare la data a partire dalla quale si prevede che la misura sia operativa. Se la misura è già operativa, si può inserire una dicitura standard (es. "misura in essere").
Periodicità e modalità dei controlli	Contiene l'indicazione della periodicità con cui sono verificate la funzionalità e l'efficienza della misura in questione.
Struttura o persone addette all'adozione	Indicare la struttura o la persona responsabili o preposte all'adozione delle misure indicate.
Riferimento alla scheda analitica	Contiene il riferimento eventuale ad una scheda analitica descrittiva della misura di sicurezza (si veda la "Scheda analitica descrittiva delle singole misure di sicurezza", illustrata qui sotto).

SCHEDA ANALITICA DESCRITTIVA DELLE SINGOLE MISURE DI SICUREZZA *(facoltativa)*

Nella bozza del DPSS, presentata nel Sito del Garante, viene precisato che può essere utile compilare, per ciascuna misura di sicurezza, una scheda analitica contenente particolareggiate informazioni, utili nella gestione operativa delle sicurezza e, in particolare, nelle attività di verifica e controllo.

Scheda numero……..
Compilata da……..
Data di compilazione…….

Misura di sicurezza	
Descrizione sintetica	
Elementi descrittivi	
Data di aggiornamento	

Il Garante precisa che queste schede sono a formato libero, e le informazioni utili devono essere decise in funzione della specifica misura. A puro titolo di esempio, potranno essere inserite informazioni relative a:

- *la minaccia che si intende contrastare*
- *la tipologia della misura di sicurezza (preventiva, di contrasto, di contenimento degli effetti…)*
- *le informazioni relative alla responsabilità della attuazione e della gestione della specifica misura*
- *i tempi di validità delle scelte adottate (contratti esterni, aggiornamento di prodotti, eccetera)*
- *gli ambiti ai quali si applica (ambiti fisici: un reparto, un edificio…., o logici: una procedura, un'applicazione…).*

ALLEGATO A) – TABELLA DI SUPPORTO AL PARAGRAFO 1.1

PRIMA COORDINATA – TIPI DI DATI TRATTATI

DATI SENSIBILI
Idonei a rivelare le origini razziali o etniche - dati idonei a rivelare l'appartenenza ad un gruppo linguistico Idonei a rivelare le convinzioni religiose; adesioni ad organizzazioni a carattere religioso Idonei a rivelare le convinzioni filosofiche o di altro genere e le adesioni ad organizzazioni a carattere filosofico Idonei a rivelare le opinioni politiche Idonei a rivelare la adesione a partiti od organizzazioni a carattere politico Idonei a rivelare la adesione a sindacati o organizzazioni a carattere sindacale Idonei a rivelare lo stato di salute - dati idonei a rivelare l'appartenenza a categorie protette - dati idonei a rivelare l'identità del donatore - dati idonei a rivelare l'identità del ricevente - dati idonei a rivelare lo stato di disabilità - dati idonei a rivelare sieropositività - dati idonei a rivelare malattie infettive e diffusive - dati idonei a rivelare malattie mentali - dati relativi a indagini epidemiologiche - dati relativi a prescrizioni farmaceutiche e cliniche - dati relativi ad esiti diagnostici e programmi terapeutici - dati relativi all'utilizzo di particolari ausili protesici - dati relativi alla prenotazione di esami clinici e visite specialistiche - dati idonei a rivelare AIDS conclamato - dati inerenti a caratteristiche o idoneità psichiche Idonei a rivelare la vita sessuale - dati idonei a rivelare lo stato di gravidanza
DATI GENETICI
Dati idonei a rilevare patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali Dati idonei a rilevare la gravità o il decorso del quadro clinico delle patologie genetiche Dati idonei a identificare malattie ereditarie Dati relativi alle malformazioni congenite la cui causa non è nota Dati idonei ad accertare maternità o paternità Dati relativi a indagini epidemiologiche Dati relativi a indagini sulla popolazione Dati relativi a trapianti di tessuti od organi o all'impiego di cellule staminali Dati relativi alla procreazione Dati tratti da studi di relazione tra patrimonio genetico e fattori di rischio
DATI BIOMETRICI
Caratteristiche della voce Geometria della mano Impronte digitali Informazioni di tipo comportamentale (andatura, movimento delle labbra, digitazione su tastiera...) Riconoscimento dell'iride o retina Rilevazione facciale attraverso uno o più elementi Combinazione di due o più elementi sopra indicati
DATI GIUDIZIARI
Dati relativi a comportamenti illeciti o fraudolenti Dati relativi a provvedimenti o procedimenti giudiziari Dati relativi a provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili
DATI DIVERSI DA QUELLI SENSIBILI E GIUDIZIARI
Nominativo, indirizzo o altri elementi di identificazione personale - nome, cognome, età, sesso, luogo e data di nascita - indirizzo privato, indirizzo di lavoro, numero di telefono, di telefax o di posta elettronica - posizione rispetto agli obblighi militari - dati fisici (altezza, peso, ecc.) - dati idonei a rivelare l'origine nazionale Codice fiscale ed altri numeri di identificazione personale

- carte sanitarie
- numero carta di identità, passaporto, patente di guida, numero di posizione previdenziale o assistenziale
- targa automobilistica

Dati relativi alla famiglia e a situazioni personali

- stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare

Istruzione e cultura

- curriculum di studi e accademico
- pubblicazioni: articoli, monografie, relazioni, materiale audio-visivo, ecc.
- titoli di studio

Lavoro

- occupazione attuale e precedente
- informazioni sul reclutamento, sul tirocinio o sulla formazione professionale
- informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione
- curriculum vitae o lavorativo, competenze professionali
- dati relativi alle pregresse esperienze professionali
- retribuzioni, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente
- dati sulla gestione e sulla valutazione delle attività lavorative
- cariche pubbliche rivestite
- dati relativi ad eventuali controversie con precedenti datori di lavoro

Beni, proprietà, possessi

- proprietà, possessi e locazioni; beni e servizi forniti o ottenuti

Attività economiche, commerciali, finanziarie e assicurative

- dati contabili, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni
- identificativi finanziari, redditi, beni patrimoniali, investimenti
- passività, solvibilità, prestiti, mutui, ipoteche
- crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi
- dati assicurativi, dati previdenziali
- dati relativi al comportamento debitorio
- dati relativi all'affidabilità o puntualità nei pagamenti
- dati relativi alla solvibilità economica
- dati relativi all'adempimento di obbligazioni
- dati relativi allo svolgimento di attività economiche e altre informazioni commerciali (es. fatturato, bilanci, aspetti economici, finanziari, organizzativi, produttivi, industriali, commerciali, imprenditoriali)
- dati relativi a comportamenti illeciti o fraudolenti
- dati relativi ad altri provvedimenti o procedimenti giudiziari
- dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili

Dati su comportamento, abitudini di vita o di consumo

- creazione di profili di utenti, consumatori, contribuenti, ecc
- profili della personalità e dei tratti caratteriali
- viaggi, spostamenti, preferenze o esigenze alimentari (eccettuate quelle fondate su convinzioni religiose o filosofiche)
- dati sull'appartenenza ad associazioni diverse da quelle di carattere religioso, filosofico, politico o sindacale
- licenze, autorizzazioni (licenze di caccia o pesca, ecc.)
- dati relativi ad attività sportive o agonistiche
- dati idonei a rivelare scelte di consumo

Dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica

- dati idonei a rilevare immagini o suoni
- dati idonei a rilevare la posizione di beni, strumenti, oggetti
- dati idonei a rilevare la posizione di persone

SECONDA COORDINATA – CATEGORIE DI SOGGETTI CUI SI RIFERISCONO I DATI TRATTATI

Abbonati
Addetti alla sicurezza
Aderenti ad associazioni politiche, religiose, sindacali o filosofiche
Agenti e rappresentanti
Agricoltori
Amministratori, coordinatori o altre persone che ricoprono incarichi in organismi di tipo associativo
Artigiani
Assistiti
Candidati a procedure concorsuali o selettive
Candidati da considerare per l'instaurazione di un rapporto di lavoro
Cittadini di Paesi appartenenti all'U.E.
Cittadini di Paesi non appartenenti all'U.E.
Cittadini italiani
Clienti o utenti (anche potenziali)
Commercianti
Concepiti e nascituri
Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione
Coniugi e conviventi
Consulenti e liberi professionisti, anche in forma associata
Consumatori
Deceduti
Donatori o riceventi
Familiari dell'interessato
Fedeli
Fornitori
Genitori
Gruppi familiari
Gruppi omogenei per abitudini sessuali
Gruppi omogenei per altre caratteristiche
Gruppi omogenei per appartenenza razziale o etnica
Gruppi omogenei per area geografica
Gruppi omogenei per caratteristiche fisiche
Gruppi omogenei per consanguineità
Gruppi omogenei per fattori di rischio
Gruppi omogenei per nazionalità
Gruppi omogenei per provenienza geografica
Imprenditori individuali, piccoli imprenditori o liberi professionisti
Indagati o imputati
Lavoratori autonomi
Lavoratori o collaboratori
Maggiori di età
Malati gravi o sottoposti a particolari trattamenti di cura
Militari o appartenenti alle forze dell'ordine
Minori di età
Neonati (entro il primo anno di vita)
Parenti, affini o conviventi
Passeggeri su veicoli o utenti di mezzi di trasporto
Pazienti, degenti o disabili
Personale dipendente
Personale pubblico dirigenziale e magistrati
Persone affette
Persone fisiche
Persone giuridiche ed altri enti (comprende societa' di persone)
Persone in cerca di occupazione
Scolari o studenti di ogni ordine e grado
Soci o associati ad associazioni o fondazioni anche non riconosciute
Soci, associati, aderenti, iscritti e simpatizzanti (anche potenziali o non più facenti parte dell'organismo di tipo associativo)

Soggetti con limitata capacità di intendere e volere Soggetti in difficoltà o pericolo (anche potenziali) Soggetti o organismi pubblici Utenti di servizi o impianti sportivi

ALLEGATO B) – Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS) – pubblicata dal Garante in data 11 giugno 2004
(Codice in materia di protezione dei dati personali art. 34 e Allegato B, regola 19, del d.lg. 30 giugno 2003, n. 196)

Premessa
La presente guida mira a facilitare l'adempimento dell'obbligo di redazione del documento programmatico sulla sicurezza (DPS) nelle organizzazioni di piccole e medie dimensioni o, comunque, non dotate al proprio interno di competenze specifiche. (*Nelle strutture di piccole dimensioni dove possono mancare specifiche competenze, si può anche consultare per alcuni profili tecnici il fornitore/installatore degli strumenti elettronici e del relativo software*).
La guida può essere di ausilio nella redazione del DPS, ma non è obbligatorio utilizzarla per adempiere all'obbligo.
La guida è strutturata in due parti: la prima contiene istruzioni per sviluppare il DPS negli aspetti descrittivi oppure nella compilazione di alcune tabelle riportate nella seconda parte.
Nella guida sono anche evidenziati altri elementi utilizzabili facoltativamente, comprese alcune tabelle, che si ritengono utili per una più approfondita definizione del DPS.

Parte I - Istruzioni

Per ciascuna regola dell'Allegato B al Codice sono riportati i contenuti, le informazioni essenziali e gli ulteriori elementi da inserire nel DPS

Elenco dei trattamenti di dati personali (regola 19.1)

Contenuti
In questa sezione sono individuati i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati. Nella redazione della lista si può tener conto anche delle informazioni contenute nelle notificazioni eventualmente inviate al Garante anche in passato.

Informazioni essenziali (vedi anche tabella 1.1)
Per ciascun trattamento vanno indicate le seguenti informazioni secondo il livello di sintesi determinato dal titolare:

- *Descrizione sintetica:* menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es., fornitura di beni o servizi, gestione del personale, ecc.) e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.).
- *Natura dei dati trattati:* indicare se, tra i dati personali, sono presenti dati sensibili o giudiziari.
- *Struttura di riferimento:* indicare la struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento. In caso di strutture complesse, è possibile indicare la macro-struttura (direzione, dipartimento o servizio del personale), oppure gli uffici specifici all'interno della stessa (ufficio contratti, sviluppo risorse, controversie sindacali, amministrazione-contabilità.)
- *Altre strutture che concorrono al trattamento:* nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture è opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.
- *Descrizione degli strumenti elettronici utilizzati:* va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi).

***Ulteriori elementi per descrivere gli strumenti (vedi anche tabella 1.2)* - da indicare facoltativamente.**

- *Identificativo del trattamento:* alla descrizione del trattamento, se ritenuto utile, può essere associato un codice, facoltativo, per favorire un'identificazione univoca e più rapida di ciascun trattamento nella compilazione delle altre tabelle.
- *Banca dati:* indicare eventualmente la banca dati (ovvero il data base o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i dati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso le banche dati potranno essere elencate.
- *Luogo di custodia dei supporti di memorizzazione:* indicare il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano (in quale sede, centrale o periferica, o presso quale fornitore di servizi, ecc.) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile. Il punto può essere approfondito meglio in occasione di aggiornamenti.

- *Tipologia di dispositivi di accesso:* elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.
- *Tipologia di interconnessione:* descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.

Le predette informazioni possono essere completate o sostituite da schemi, tabelle, disegni di architettura del sistema informativo o da altri documenti aziendali già compilati e idonei a fornire in altro modo le informazioni medesime.

Distribuzione dei compiti e delle responsabilità (regola 19.2)
Contenuti
In questa sezione occorre descrivere sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati. Si possono utilizzare anche mediante specifici riferimenti documenti già predisposti (provvedimenti, ordini di servizio, regolamenti interni, circolari), indicando le precise modalità per reperirli.
Informazioni essenziali (vedi anche tabella 2)

- *Struttura:* riportare le indicazioni delle strutture già menzionate nella precedente sezione.
- *Trattamenti effettuati dalla struttura:* indicare i trattamenti di competenza di ciascuna struttura.
- *Compiti e responsabilità della struttura:* descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.). Anche in questo caso è possibile utilizzare, nei termini predetti, altri documenti già predisposti.

Analisi dei rischi che incombono sui dati (regola 19.3)
Contenuti
Descrivere in questa sezione i principali eventi potenzialmente dannosi per la sicurezza dei dati, e valutarne le possibili conseguenze e la gravità in relazione al contesto fisico–ambientale di riferimento e agli strumenti elettronici utilizzati.
Informazioni essenziali (vedi anche tabella 3)

- *Elenco degli eventi:* individuare ed elencare gli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali. In particolare, si può prendere in considerazione la lista esemplificativa dei seguenti eventi:
  1) comportamenti degli operatori:
  - sottrazione di credenziali di autenticazione
  - carenza di consapevolezza, disattenzione o incuria
  - comportamenti sleali o fraudolenti
  - errore materiale

  2) eventi relativi agli strumenti:
  - azione di virus informatici o di programmi suscettibili di recare danno
  - spamming o tecniche di sabotaggio
  - malfunzionamento, indisponibilità o degrado degli strumenti
  - accessi esterni non autorizzati
  - intercettazione di informazioni in rete

  3) eventi relativi al contesto fisico-ambientale:
  - ingressi non autorizzati a locali/aree ad accesso ristretto
  - sottrazione di strumenti contenenti dati
  - eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria
  - guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
  - errori umani nella gestione della sicurezza fisica

  E' possibile, per ulteriori dettagli, rinviare a documenti analoghi già redatti in tema di piani di sicurezza e gestione del rischio, come ad es.: *Business Continuity Plan*, *Disaster Recovery Plan*, ecc. (si tenga però presente che le analisi alla base di questi altri documenti possono avere una natura ben diversa).
- *Impatto sulla sicurezza:* descrivere le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento, e valutare la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'evento (anche in termini sintetici: es., alta/media/bassa). In questo modo è possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare.

L'analisi dei rischi può essere condotta utilizzando metodi di complessità diversa: l'approccio qui descritto è volto solo a consentire una prima riflessione in contesti che per dimensioni ridotte o per altre analoghe ragioni, non ritengano di dover procedere ad una analisi più strutturata.

Misure in essere e da adottare (regola 19.4)

Contenuti

In questa sezione vanno riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia. Le misure da adottare possono essere inserite in una sezione dedicata ai programmi per migliorare la sicurezza.

Informazioni essenziali

- *Misure:* descrivere sinteticamente le misure adottate (seguendo anche le indicazioni contenute nelle altre regole dell'Allegato B del Codice).
- *Descrizione dei rischi:* per ciascuna misura indicare sinteticamente i rischi che si intende contrastare (anche qui, si possono utilizzare le indicazioni fornite dall'Allegato B).
- *Trattamenti interessati:* indicare i trattamenti interessati per ciascuna delle misure adottate. Determinate misure possono non essere riconducibili a specifici trattamenti o banche di dati (ad esempio, con riferimento alle misure per la protezione delle aree e dei locali). Occorre specificare se la misura è già in essere o da adottare, con eventuale indicazione, in tale ultimo caso, dei tempi previsti per la sua messa in opera.
- *Struttura o persone addette all'adozione:* indicare la struttura o la persona responsabili o preposte all'adozione delle misure indicate.

***Ulteriori elementi per la descrizione analitica delle misure di sicurezza (vedi anche tabella 4.2)* - da indicare facoltativamente.**

Oltre alle informazioni sopra riportate può essere opportuno compilare, per ciascuna misura, una scheda analitica contenente un maggior numero di informazioni, utili nella gestione operativa della sicurezza e, in particolare, nelle attività di verifica e controllo.

Queste schede sono a formato libero e le informazioni utili devono essere individuate in funzione della specifica misura. A puro titolo di esempio, possono essere inserite informazioni relative a:

- la minaccia che si intende contrastare
- la tipologia della misura (preventiva, di contrasto, di contenimento degli effetti ecc.)
- le informazioni relative alla responsabilità dell'attuazione e della gestione della misura
- i tempi di validità delle scelte (contratti esterni, aggiornamento di prodotti, ecc.)
- gli ambiti cui si applica (ambiti fisici -un reparto, un edificio, ecc.– o logici - una procedura, un'applicazione, ecc.)

Può essere opportuno indicare chi ha compilato la scheda e la data in cui la compilazione è terminata.

Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

Contenuti

In questa sezione sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci. Pertanto, è opportuno descrivere sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino.

Informazioni essenziali (vedi anche tabella 5.1)

Per quanto riguarda il ripristino, le informazioni essenziali sono:

- *Banca dati/Data base/Archivio:* indicare la banca dati, il data base o l'archivio interessati.
- *Criteri e procedure per il salvataggio e il ripristino dei dati:* descrivere sinteticamente le procedure e i criteri individuati per il salvataggio e il ripristino dei dati, con eventuale rinvio ad un'ulteriore scheda operativa o a documentazioni analoghe.
- *Pianificazione delle prove di ripristino*: indicare i tempi previsti per effettuare i test di efficacia delle procedure di salvataggio/ripristino dei dati adottate.

***Ulteriori elementi per specificare i criteri e le procedure per il salvataggio e il ripristino dei dati (vedi anche tabella 5.2)* - da indicare facoltativamente**

- *Data base:* identificare la banca, la base o l'archivio elettronico di dati interessati.
- *Criteri e procedure per il salvataggio dei dati:* descrivere sinteticamente la tipologia di salvataggio e la frequenza con cui viene effettuato.
- *Modalità di custodia delle copie:* indicare il luogo fisico in cui sono custodite le copie dei dati salvate.
- *Struttura o persona incaricata del salvataggio:* indicare la struttura o le persone incaricate di effettuare il salvataggio e/o di controllarne l'esito.

Pianificazione degli interventi formativi previsti (regola 19.6)

Contenuti

In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

Informazioni essenziali

- *Descrizione sintetica degli interventi formativi:* descrivere sinteticamente gli obiettivi e le modalità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 (ingresso in servizio o cambiamento di mansioni degli incaricati, introduzione di nuovi elaboratori, programmi o sistemi 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, anche in riferimento alle strutture di appartenenza.
- *Tempi previsti:* indicare i tempi previsti per lo svolgimento degli interventi formativi.

Trattamenti affidati all'esterno (regola 19.7)

Contenuti

Redigere un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Informazioni essenziali

- *Descrizione dell'attività "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 cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento).
- *Descrizione dei criteri:* perché sia garantito un adeguato trattamento dei dati è necessario che la società a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento, ad esempio, a:
  1. trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
  2. adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
  3. rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
  4. impegno a relazionare periodicamente sulle misure di sicurezza adottate –anche mediante eventuali questionari e liste di controllo- e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

Contenuti

In questa sezione vanno rappresentate le modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura, o la separazione fra dati identificativi e dati sensibili, nonché i criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti. Questo punto riguarda solo organismi sanitari e esercenti professioni sanitarie (regola 24).

Informazioni essenziali

- *Trattamenti di dati:* descrivere i trattamenti (le banche o le basi di) dati oggetto della protezione
- *Protezione scelta:* riportare la tipologia di protezione adottata, scelta fra quelle indicate dal Codice o in base a considerazioni specifiche del titolare.
- *Tecnica adottata:* descrivere sinteticamente, in termini tecnici ed eventualmente organizzativi, la misura adottata. Ad esempio, in caso di utilizzo di cifratura, le modalità di conservazione delle chiavi e le procedure di utilizzo.

Parte II - Tabelle

Per ciascuna regola sono riportate, di seguito, una o più tabelle. Le istruzioni per la compilazione dei campi che le compongono è contenuta nella Parte I. Per ciascuna tabella può essere indicata facoltativamente anche la data di compilazione, che può rivelarsi utile qualora la tabella sia compilata in data significativamente diversa (antecedente) rispetto alla redazione finale del DPS.

Tabella 1.1 – Elenco dei trattamenti: informazioni essenziali
Data di compilazione (*facoltativa*): ……..

	TRATTAMENTO 1	**TRATTAMENTO 2**	**TRATTAMENTO n**
Descrizione sintetica del trattamento			
- Finalità perseguita o attività svolta			
- Categorie di interessati			
Natura dei dati trattati:			
- Comuni			
- Sensibili			
- Giudiziari			
Struttura di riferimento			
Altre strutture (anche esterne) che concorrono al trattamento			
Descrizione degli strumenti utilizzati			

Tabella 1.2 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti 2
Da compilare facoltativamente, collegandola alla tabella precedente, ad esempio attraverso l'identificativo.
Data di compilazione (*facoltativa*): ……..

	TRATTAMENTO 1	**TRATTAMENTO 2**	**TRATTAMENTO n**
Identificativo del trattamento			
Eventuale banca dati			
Ubicazione fisica dei supporti di memorizzazione			
Tipologia di dispositivi di accesso			
Tipologia di interconnessione			

Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti
Data di compilazione (*facoltativa*): ……..

	STRUTTURA 1	**STRUTTURA 2**	**STRUTTURA n**
Struttura			
Trattamenti effettuati dalla struttura			
Descrizione dei compiti e delle responsabilità della struttura			

Tabella 3 - Analisi dei rischi
Data di compilazione (*facoltativa*): ……..

Rischi	SI/NO	Descrizione dell'impatto sulla sicurezza (gravità: alta / media / bassa)
Comportamenti 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 *virus* informatici o di programmi suscettibili di recare danno		
Spamming 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, ...)		
Errori umani nella gestione della sicurezza fisica		
Altro evento		

Tabella 4.1 – Le misure di sicurezza adottate o da adottare
Data di compilazione (*facoltativa*): ……..

	MISURA 1	MISURA 2	MISURA n
Misure			
Descrizione dei rischi contrastati			
Trattamenti interessati			
Specificare se			
▪ Misura già in essere			
▪ Misura da adottare - *Indicare eventualmente i tempi previsti per l'adozione delle misure*			
Strutture o persone addette all'adozione			

Tabella 4.2 - Scheda descrittiva delle misure adottate
Da compilare facoltativamente.
Data di compilazione (*facoltativa*): ……..
Scheda numero:……..
Compilata da:……

Misura	
Descrizione sintetica	
Elementi descrittivi	
Data aggiornamento	

Tabella 5.1 - Criteri e procedure per il ripristino della disponibilità dei dati
Data di compilazione (*facoltativa*): ……..

Ripristino	**DATA BASE 1**	**DATA BASE 2**	**DATA BASE n**
Banca / database / archivio di dati			
Criteri e procedure per il salvataggio e il ripristino dei dati			
Pianificazione delle prove di ripristino			

Tabella 5.2 - Criteri e procedure per il salvataggio dei dati
Da compilare facoltativamente.
Data di compilazione (*facoltativa*): ……..

Salvataggio	**DATA BASE 1**	**DATA BASE 2**	**DATA BASE n**
Banca dati			
Criteri e procedure per il salvataggio			
Luogo di custodia delle copie			
Struttura o persona incaricata del salvataggio			

Tabella 6 - Pianificazione degli interventi formativi previsti
Data di compilazione (*facoltativa*): ……..

	CORSO 1	**CORSO 2**	**CORSO n**
Descrizione sintetica degli interventi formativi			
Classi di incarico o tipologie di incaricati interessati			
Tempi previsti			

Tabella 7 - Trattamenti affidati all'esterno
Data di compilazione (*facoltativa*): ……..

	ATTIVITA' 1	**ATTIVITA' 2**	**ATTIVITA' n**
Descrizione sintetica dell'attività esternalizzata			
Trattamenti di dati interessati			
Soggetto esterno			
Descrizione dei criteri e degli impegni assunti per l'adozione delle misure			

Tabella 8 - Cifratura dei dati o separazione dei dati identificativi
Solo per organismi sanitari ed esercenti professioni sanitarie).
Data di compilazione (*facoltativa*): ……..

	DATO 1	**DATO 2**	**DATO n**
Trattamenti di dati			
Protezione scelta (Cifratura / Separazione)			
Tecnica adottata			
- Descrizione			
- Informazioni utili			

DOCUMENTO REDATTO AI SENSI E PER GLI EFFETTI DI CUI ALL'ARTICOLO 180 DLGS 196/2003 PER BENEFICIARE DEL PIU' LUNGO TERMINE DEL 31 DICEMBRE 2004, INVECE DI QUELLO ORDINARIO DEL 30 GIUGNO 2004, PER ADOTTARE LE NUOVE MISURE DI SICUREZZA, INTRODOTTE DAL DLGS 196/2003 E DAL DISCIPLINARE TECNICO AD ESSO ALLEGATO SUB B)

Il titolare del trattamento…….., con sede in…….., codice fiscale……., redige il presente documento per beneficiare di quanto disposto dai commi 2 e 3 dell'articolo 180 decreto legislativo 30 giugno 2003, n. 196 (in seguito, "codice privacy"), che ha approvato il codice in materia di protezione dei dati personali.
Per i trattamenti effettuati con l'utilizzo di strumenti elettronici, tale norma concede la facoltà di completare il processo di adozione delle nuove misure minime di sicurezza, introdotte dall'articolo 34 del codice privacy e dalle relative modalità tecniche previste dall'allegato B) al codice privacy, entro un anno dalla entrata in vigore del codice privacy (quindi entro il 31 dicembre 2004), invece che entro il 30 giugno 2004.
Il più lungo termine è concesso per i trattamenti effettuati con strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione, dal 1° gennaio 2004, delle nuove misure minime di sicurezza, introdotte dal codice privacy e dal relativo disciplinare tecnico (allegato B al codice privacy).

Si descrivono nel seguito gli strumenti elettronici inadeguati, spiegando, per ciascuno di essi:
- le ragioni per cui è inadeguato
- gli interventi previsti, per renderlo adeguato alla nuova normativa privacy
- i tempi previsti, che dovranno in ogni caso permettere l'adozione delle nuove misure minime di sicurezza entro il 31 dicembre 2004
- le spese previste, in linea di massima, per procedere all'adeguamento.

Indice **Pag.**

1	La descrizione degli strumenti elettronici tecnicamente inadeguati	
2	Le ragioni dell'inadeguatezza tecnica	
3	Gli interventi previsti per procedere all'adeguamento	
4	I tempi dell'adeguamento	
5	Le spese previste	
6	Dichiarazione finale di impegno	

1. La descrizione degli strumenti elettronici tecnicamente inadeguati

Per la distinzione tra le diverse categorie di elaboratori e di strumenti elettronici, si veda il paragrafo 3.2.1 del manuale.

1° caso

Elaboratore non in rete, né dotato di accesso ad Internet, prodotto da……., anno di acquisto……

2° caso

Strumenti elettronici collegati tra loro tramite rete non disponibile al pubblico, composta da……server, ……..terminali, …….stampanti, ……altri strumenti elettronici, entrata in funzione nell'anno…….

3° caso

Elaboratore non in rete con altri, ma dotato di accesso ad Internet, prodotto da……., anno di acquisto…….

4° caso

Strumenti elettronici collegati tra loro tramite rete disponibile, anche in parte, al pubblico, composta da……server, ……..terminali, …….stampanti, ……altri strumenti elettronici, entrata in funzione nell'anno…….

2. Le ragioni dell'inadeguatezza tecnica

L'elaboratore descritto / le rete di strumenti elettronici descritta non è risultato tecnicamente adeguato, in data 1° gennaio 2004, per consentire di adottare le nuove misure minime di sicurezza previste dal codice privacy, e dal relativo disciplinare tecnico, per le seguenti ragioni (*indicare quella, anche più di una, che si applica al caso in esame*):

- l'elaboratore / la rete di strumenti elettronici non consente di adottare un sistema di autenticazione informatica, che rispetti le prescrizioni dettate dai punti da 1. a 11. del disciplinare tecnico (s*i veda il paragrafo 6.1 del manuale*)
- l'elaboratore non permette di assegnare individualmente una parola chiave a ciascun incaricato che lavora con esso, come prescritto dal punto 2. del disciplinare tecnico (*la motivazione è valida solo per il **1° caso**. Si veda il paragrafo 6.1 del manuale*)
- la rete di strumenti elettronici permette un solo livello di accesso, per la funzione di amministratore del sistema, per cui ai soggetti che rivestono tale ruolo non è possibile assegnare individualmente una parola chiave, come prescritto dal punto 2. del disciplinare tecnico (*la motivazione è valida solo per il **2° caso** ed il **4° caso**. Si veda il paragrafo 6.1 del manuale*)
- l'elaboratore / la rete di strumenti elettronici non permette di adottare un sistema di autorizzazione, per il trattamento dei dati personali, come richiesto dal punto 12. del disciplinare (*la motivazione è valida per **tutti e quattro i casi**, con l'eccezione delle ipotesi in cui si trattino dati sensibili o giudiziari con le modalità **3° caso** e **4° caso**. Si veda il paragrafo 6.2 del manuale*)
- l'elaboratore non supporta il caricamento di un aggiornato sistema antivirus, come richiesto dal punto 16. del disciplinare (*la motivazione è valida solo per **il 1° caso**. Si veda il paragrafo 6.3.1 del manuale)*
- l'elaboratore / la rete di strumenti elettronici non sono dotati di strumenti elettronici atti a proteggerli contro l'accesso abusivo, di cui all'articolo 615-ter del codice penale, come richiesto dal punto 20. del disciplinare (*la motivazione è valida solo per il **2° caso**, **3° caso** e **4° caso**, limitatamente alle ipotesi in cui si trattino dati sensibili o giudiziari. Si veda il paragrafo 6.3.1 del manuale*)
- l'elaboratore / la rete di elaboratori non supporta il caricamento di programmi volti a prevenire la vulnerabilità degli strumenti elettronici, e a correggerne difetti, come richiesto dal punto 17. del disciplinare (*la motivazione è valida per **tutti e quattro i casi**. Si veda il paragrafo 6.3.1 del manuale)*

3. Gli interventi previsti per procedere all'adeguamento

Per adeguare l'elaboratore / gli strumenti elettronici a quanto previsto dal nuovo codice privacy, è necessario procedere ai seguenti interventi (*indicare quello, anche più di uno, che si applica al caso in esame*):

- sostituzione con strumenti più aggiornati
- aggiunta delle seguenti componenti hardware:
- aggiunta delle seguenti componenti software:
- sostituzione delle seguenti componenti:……..ed aggiunta delle seguenti componenti hardware / software:…...

4. I tempi dell'adeguamento

Si prevede la seguente tempistica, per l'effettuazione degli interventi:

- i nuovi strumenti / i componenti hardware / i componenti software aggiunti verranno installati entro il mese di ….2004
- il piano di istruzione del personale, per l'utilizzo dei nuovi strumenti, verrà completato entro il mese di…..2004
- in ogni caso, entro il dicembre 2004 i nuovi strumenti / i componenti hardware / i componenti software aggiunti saranno pienamente operativi.

5. Le spese previste

Il preventivo di massima, per procedere agli interventi, è pari ad euro…….complessivi, di cui euro……..per l'acquisto di nuovi strumenti elettronici, o l'aggiornamento di quelli già esistenti, cui si aggiungono euro…..per gli interventi formativi del personale.

6. Dichiarazione finale di impegno

Durante il periodo necessario, per procedere all'adeguamento, verrà adottata ogni possibile misura di sicurezza, in relazione agli strumenti elettronici detenuti, in modo da evitare, anche sulla base di idonee misure organizzative, logistiche e procedurali, un incremento dei rischi di distruzione o perdita, anche accidentale, dei dati personali oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

==========

Al presente documento, redatto su carta intestata del Titolare, e firmato dal Titolare stesso / dal rappresentante legale del Titolare *Nome Cognome*……., viene attribuita data certa mediante l'adozione dei seguenti accorgimenti (*scegliere uno o più*):

- ricorso alla c.d. "autoprestazione" presso uffici postali prevista dall'art. 8 del d.lg. 22 luglio 1999, n. 261, con apposizione del timbro direttamente sul documento avente corpo unico, anziché sull'involucro che lo contiene
- (*per le amministrazioni pubbliche*) adozione di un atto deliberativo di cui sia certa la data in base alla disciplina della formazione, numerazione e pubblicazione dell'atto
- apposizione della c.d. marca temporale sui documenti informatici (art. 15, comma 2, legge 15 marzo 1997, n. 59; d.P.R. 10 novembre 1997, n. 513; artt. 52 ss. d.P.C.M. 8 febbraio 1999)
- apposizione di autentica, deposito del documento o vidimazione di un verbale, in conformità alla legge notarile; formazione di un atto pubblico
- registrazione o produzione del documento a norma di legge presso un ufficio pubblico.

Esso verrà successivamente conservato presso il Titolare, per esibirlo in caso di eventuali controlli, da parte delle Autorità competenti.

Data e firma