GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# *Prime riflessioni sui criteri di redazione*

# *del*

# *Documento programmatico sulla sicurezza*

*(art. 34 e regola 19 dell'Allegato B*

*del Codice in materia di protezione dei dati personali)*

Bozza del 13 maggio 2004

## Indice

## *Premessa*

*Questo documento è frutto delle riflessioni di un gruppo di lavoro di esperti della sicurezza che ha fornito un contributo ora aperto a suggerimenti, proposte ed eventuali critiche al fine di perfezionarlo, entro il mese di maggio. Si avrà così una guida operativa, con alcune istruzioni e tabelle fac-simile, per redigere un documento programmatico sulla sicurezza (Dps) quando questo è necessario, a pena di sanzioni penali, ai sensi della regola 19 dell'Allegato B del Codice.*

*Il contributo mira, in particolare, a facilitare l'adempimento dell'obbligo da parte delle organizzazioni di piccole e medie dimensioni o, comunque, non dotate al proprio interno di competenze specifiche.*

*La guida dovrebbe essere d'ausilio alla redazione del Dps ma non costituirà un riferimento obbligato per chi deve ottemperare alla regola 19.*

***Struttura generale del documento***

*Per ogni regola sono riportate, di seguito, una o più tabelle precedute dalla descrizione dei campi che le compongono.*

*Ogni tabella riporta una data di compilazione che può essere utile se la tabella è compilata in data significativamente diversa (antecedente) rispetto alla redazione finale del Dps.*

## Elenco dei trattamenti di dati personali (regola 19.1)

***Contenuti.***

In questa sezione deve essere inserito l'elenco dei trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati trattati e della struttura (o reparto, funzione, ufficio, ...) interna od esterna che operativamente effettua il trattamento. Nella redazione della lista può essere utile fare riferimento anche alle informazioni contenute nelle notificazioni eventualmente inviate al Garante anche in passato.

***Informazioni essenziali.***

Per ciascun trattamento è riportate le seguenti informazioni:

*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 altre tabelle

*Descrizione sintetica:* descrive il trattamento in modo da consentire una comprensione immediata della tabella.

*Natura dei dati trattati:* dovrà essere indicato se, tra i dati oggetto del singolo trattamento elencato, sono presenti dati sensibili o giudiziari, oltre ad altri dati personali.

*Struttura di riferimento:* indica la struttura (o reparto, funzione, ufficio, ecc.) all'interno della quale viene realizzato il trattamento. Il livello di sintesi utilizzato è stabilito dal titolare. Ad esempio, in caso di strutture complesse, è possibile indicare la macro-struttura (direzione del personale) oppure uffici specifici (uff. paghe, ufficio sviluppo risorse, ufficio controversie sindacali, ecc.)

*Altre funzioni che concorrono al trattamento:* nel caso in cui un trattamento, per essere completato, comporti l'attività di diverse strutture è opportuno indicare oltre quella che primariamente detiene la responsabilità dell'attività, anche quelle che concorrono, siano esse interne od esterne all'organizzazione del titolare.

*Banca dati:* il nome o l'identificativo dell'eventuale banca dati (ovvero del data base o dell'archivio informatico) in cui sono contenuti i dati che sono trattati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso elencare le banche.

*Ubicazione fisica dei supporti di memorizzazione:* contiene l'indicazione del luogo in cui risiedono fisicamente i dati, cioè dove si trova (in quale sede, centrale o periferica, presso quale fornitore di servizi, etc.) l'elaboratore sui cui dischi sono memorizzati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, Cd, ecc.). Il livello di dettaglio deve essere funzionale alla esigenze della politica della sicurezza da definire.

*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 informatica che collega i dispositivi d'accesso utilizzati dagli incaricati ai dati: rete locale, Extranet, Internet, ecc.

***Tabella 1.1. Elenco dei trattamenti: informazioni di base.***

| Identificativo del Trattamento | Descrizione sintetica | Natura dei dati trattati | | Struttura di riferimento | Altre strutture (anche esterne) che concorrono al trattamento | Descrizione degli strumenti utilizzai |
|---|---|---|---|---|---|---|
| | | S | G | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| Data di aggiornamento: | | | | | | |

***Tabella 1.2. Elenco dei trattamenti: descrizione degli strumenti utilizzati***

| Identificativo del trattamento | Eventuale banca dati | Ubicazione fisica dei supporti di memorizzazione | Tipologia di dispositivi di accesso | Tipologia di interconnessione |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| Data di aggiornamento: | | | | |

## Distribuzione dei compiti e delle responsabilità (regola 19.2)

### *Contenuti.*

In questa sezione è costruita una mappa che associa ad ogni struttura (o reparto, dipartimento, ufficio) i trattamenti da questa effettuati, descrivendo sinteticamente l'organizzazione della struttura medesima e le relative responsabilità. Ci si può riferire anche ad analoghe documentazioni già predisposte dal titolare (ordinamenti, ordini di servizio, regolamenti interni).

***Informazioni essenziali.***

*Struttura aziendale:* contiene lo stesso identificativo utilizzato nella sezione precedente.

*Responsabile della struttura:* indica il ruolo o la qualifica del dirigente o del responsabile della struttura (non deve essere confuso il responsabile del trattamento ai sensi dell'art. 29).

*Trattamenti operati dalla struttura:* contiene, se necessario su più righe per ciascuna struttura, i trattamenti per i quali la struttura ha la primaria responsabilità.

*Compiti della struttura:* contiene una descrizione sintetica dei compiti assegnati alla 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, ecc.).

***Tabella 2.1. Strutture preposte ai trattamenti.***

| Struttura | Responsabile | Trattamenti operati dalla struttura | Compiti della struttura |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Data di aggiornamento: | | | |

## Analisi dei rischi che incombono sui dati (regola 19.3)

***Contenuti***

Individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutarne le possibili conseguenze e la gravità e porli in correlazione con misure previste.

***Informazioni essenziali***

*Elenco degli eventi:* contiene l'elenco degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali. L'elenco identifica pertanto diversi eventi che possono rilevare per l'analisi dei rischi per la sicurezza dei dati personali. Nella tabella riportata nel seguito è proposta una lista esemplificativa di eventi, da prendere in considerazione eventualmente solo come base di partenza.

*Impatto sulla sicurezza dei dati:* contiene la descrizione delle principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento ed una valutazione della gra-

vità delle stesse, anche in relazione alla probabilità stimata dell'evento. In questo modo consente di formulare un indicatore qualitativo di gravità omogeneo per i diversi eventi che deve essere esplicitato.

*Rif. misure d'azione:* contiene il riferimento alla contromisura adottata.

*Nota: l'analisi dei rischi può essere condotta utilizzando metodi di complessità diversa. L'approccio descritto vuole consentire una prima riflessione in contesti che, per dimensioni, per complessità organizzativa ridotta o per altre ragioni, non richiedano analisi più articolate.*

Nel seguito è riportata una tabella che può facilitare l'organizzazione delle informazioni richieste.

***Tabella 3.1. Analisi dei rischi***

| Evento | | Impatto sulla sicurezza dei dati | | Rif. misure d'azione |
|---|---|---|---|---|
| Comportamenti degli operatori | furto di credenziali di autenticazione | Descrizione | Gravità stimata | |
| | carenza di consapevolezza, disattenzione o incuria | | | |
| | comportamenti sleali o fraudolenti | | | |
| | errore materiale | | | |
| Eventi relativi agli strumenti | azione di *virus* informatici o di codici malefici | | | |
| | *spamming* o altre tecniche di sabotaggio | | | |
| | malfunzionamento, indisponibilità o degrado degli strumenti | | | |
| | accessi esterni non autorizzati | | | |
| | intercettazione di informazioni in rete | | | |
| Eventi relativi al contesto | accessi non autorizzati a locali/reparti ad accesso ristretto | | | |
| | asportazione e furto di strumenti contenenti dati | | | |
| | eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria | | | |
| | guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...) | | | |
| | errori umani nella gestione della sicurezza fisica | | | |

## Misure in essere e da adottare (regola 19.4).

### *Contenuti*

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 qui 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. Senza procedure di controllo periodico, infatti, nessuna misura può essere considerata completa.

Le misure da adottare possono essere inserite anche in una apposita sezione dedicata ai programmi di miglioramento della sicurezza.

### *Informazioni essenziali.*

*Misure:* la descrizione sintetica della misura di sicurezza adottata.

*Rischio contrastato:* per ogni misura è necessario indicare il riferimento all'elemento dell'analisi dei rischi che ha motivato l'adozione della misura in oggetto.

*Data base/trattamento interessato:* riportare l'identificativo del (dei) *data base* o dell'archivio informatizzato e dei trattamenti interessati per ciascuna delle misure adottate

È da notare che determinate misure possono non essere riconducibili a specifici trattamenti o basi di dati.

*Rif. Scheda analitica:* contiene il riferimento eventuale ad una scheda analitica descrittiva della misura, eventualmente compilata anche utilizzando la successiva tabella 4.2.

*Data di effettività*: per ogni misura è necessario indicare la data a partire dalla quale la misura è operativa o se già operativa una dicitura *standard* (ad es.: "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 e della struttura operativa che ne ha la responsabilità.

### *Informazioni descrittive analitiche delle misure di sicurezza*

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

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, ecc.)

- gli ambiti a cui si applica (ambiti fisici: un reparto, un edificio, ... – o logici: una procedura, un'applicazione, ...)
- ...

È comunque opportuno mantenere l'indicazione di chi ha compilato la scheda e della data in la compilazione è stata terminata.

Nel seguito sono riportate due tabelle che possono facilitare l'organizzazione delle informazioni richieste.

***Tab. 4.1. Le misure di sicurezza adottate o da adottare***

| Misura | Rischio contrastato | Trattamento interessato | Eventuale banca dati interessata | Rif. scheda analitica | Misura già in essere | Misura da adottare (*) | Periodicità e responsabilità dei controlli |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Data aggiornamento: | | | | | | | |

*(*) Indicare anche la data se individuata*

***Tab. 4.2. Scheda descrittiva delle misure adottate***

| Scheda nr. | | Compilata da | | Data di compilazione | |
|---|---|---|---|---|---|
| Misura | | | | | |
| Descrizione sintetica | | | | | |
| Elementi descrittivi | | | | | |
| | | | | | |
| Data aggiornamento: | | | | | |

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

### *Contenuti*

In questa sezione sono descritti i criteri e le procedure adotti per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva direttamente dalla eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che quando sono necessarie le copie dei dati siano disponibili e le procedure efficaci.

### *Informazioni essenziali.*

*Data base:* contiene l'identificativo del data base o dell'archivio interessato.

*Dati sensibili o giudiziari contenuti:* contiene l'elenco dei dati sensibili o giudiziari contenuti nel database o archivio.

*Criteri individuati per il salvataggio (procedure operative in essere):* contiene una descrizione della tipologia di salvataggio e della frequenza con cui viene effettuato.

*Ubicazione di conservazione delle copie:* contiene l'indicazione del luogo fisico in cui sono custodite le copie dei dati salvate.

*Struttura operativa o persona incaricata del salvataggio:* contiene il nominativo della persona incaricata di effettuare il salvataggio e/o di controllarne l'esito o del coordinatore del gruppo preposto.

***Tab. 5.1.***

| Salvataggio | | | | | |
|---|---|---|---|---|---|
| Data base | Dati sensibili o giudiziari contenuti | Criteri individuati per il salvataggio (procedure operative in essere) | | Ubicazione di conservazione delle copie | Struttura operativa incaricata del salvataggio |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Data di aggiornamento | | | | | |

Per quanto riguarda il ripristino, le informazioni essenziali sono le seguenti:

*Data base/archivio:* contiene l'identificativo del *data base* o dell'archivio interessato.

*Scheda operativa:* contiene il riferimento alla scheda operativa che descrive la procedura di ripristino

*Pianificazione delle prove di ripristino:* contiene l'indicazione delle date in cui si prevede di effettuare dei *test* di efficacia delle procedure i salvataggio/ripristino dei dati adottate.

***Tab. 5.2.***

| Rispristino | | |
|---|---|---|
| Data base/archivio | Scheda operativa | Pianificazione delle prove di ripristino |
| | | |
| | | |
| Data aggiornamento: | | |

## Pianificazione degli interventi formativi previsti (regola 19.6)

### *Contenuti*

In questa sezione sonoriportate le informazioni necessarie per disporre di un quadro sintetico dell'impegno formativo che si prevede di sostenere in attuazione della normativa.

### *Informazioni essenziali.*

*Corso di formazione:* riporta l'identificativo del corso di formazione.

*Descrizione sintetica:* contiene la descrizione sintetica degli obiettivi del corso.

*Classi di incarico interessate:* contiene l'elenco delle classi omogenee di incarico a cui il corso è destinati e/o le tipologie di incaricati interessati.

*Numero di incaricati interessati:* contiene il numero di addetti interessati dal corso.

*Numero di incaricati già formati/da formare nell'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.

***Tab. 6.1.***

| Corso di formazione | Descrizione sintetica | Classi di incarico interessate | Numero di incaricati interessati | Numero di incaricati già formati/da formare nell'anno | Calendario |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Data aggiornamento: | | | | | |

## Trattamenti affidati all'esterno (regola 19.7)

### *Contenuti*

Obiettivo di questa sezione è redigere un quadro sintetico delle attività trasferite a terzi che comportano il trattamento di dati personali con l'indicazione sintetica del quadro contrattuale in cui tale trasferimento si inserisce, in riferimento alla protezione dei dati personali.

### *Informazioni essenziali*

*Attività delegata:* contiene l'identificativo dell'attività che è stata oggetto di delega a terzi.

*Descrizione sintetica:* contiene una descrizione sintetica dell'attività.

*Dati personali, sensibili o giudiziari interessati:* contiene l'elenco dei dati personali, sensibili o giudiziari oggetto di trattamento per la realizzazione dell'attività delegata.

*Soggetto delegat*o: riporta l'identificativo della società o del consulente a cui è stato affidato l'incarico.

*Descrizione dei criteri per garantire l'adozione delle misure:* perché sia garantito un adeguato trattamento dei dati è necessario che il soggetto esterno a cui viene affidato il trattamento si assuma alcuni impegni su base contrattuale.

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 del codice per la protezione dei dati personali;

2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali

3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.

4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare 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.

In questa casella sono riportati gli impegni contrattualmente assunti nel caso specifico.

*Date delle verifiche:* contiene l'indicazione del numero e delle date delle verifiche previste.

***Tab. 7.1.***

| Attività esternalizzata | Descrizione sintetica | Dati personali, sensibili o giudiziari interessati | Soggetto esterno | Descrizione dei criteri per l'adozione delle misure |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Data di aggiornamento: | | | | |

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

***Contenuti.***

In questa sezione devono essere rappresentate le modalità di protezione adottate per i dati per cui è richiesta la cifratura o la separazione fra dati identificativi e dati personali, nonché i criteri e le modalità con le quali viene assicurata la sicurezza di tali trattamenti.

Si ricorda che questo punto riguarda gli organismi sanitari e gli esercenti professioni sanitarie (art. 24).

***Informazioni essenziali.***

*Dato:* contiene l'identificativo di un insieme di informazioni personali tra loro coerenti.

*Protezione scelta:* riporta la tipologia di protezione adottata, scelta fra quelle indicate dal Codice o in base a considerazioni specifiche del titolare.

*Data di effettività*: contiene la data a partire dalla quale le misure adottate sono diventate operative.

*Tecnica adottata:* contiene una descrizione sintetica tecnica ed eventualmente organizzativa della misura adottata. Ad esempio, in caso di utilizzo di crittografia, le modalità di conservazione delle chiavi e le procedure di utilizzo delle stesse.

***Tab. 8.1.***

| Dato | Protezione scelta (Cifratura/Separazione) | Data di effettività | Tecnica adottata | |
|---|---|---|---|---|
| | | | Descrizione | Informazioni utili |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Data aggiornamento: | | | | |