Mini guida al DOCUMENTO PROGRAMMATICO SICUREZZA

(dlg.196/2003)

A cura di Gabriele Cappelletti

INDICE

1 SCOPO DI QUESTO DOCUMENTO

1.1 PREMESSA

Questo documento vuole riassumere e raccogliere le problematiche legate alla sicurezza dei dati personali conservati da una piccola o media (o micro) impresa e vuole analizzare in sintesi le informazione necessarie per redigere in modo soddisfacente un documento programmatico sulla sicurezza (D.P.S. o D.P.S.S.).
Si ricorda che il D.P.S. è una **misura minima** necessaria definita dalla legge sulla Privacy, ma è anche un'occasione per fare chiarezza all'interno della propria azienda su una serie di problematiche altrimenti spesso trattate con sufficienza e scarsa attenzione. Per questo è importante che il documento venga:

- redatto internamente, oppure,
- affidato a consulenti o fornitori esterni di fiducia con i quali collaborare alla raccolta dei dati e ai modi per descrivere il proprio sistema

In questo secondo caso è necessario sottolineare che la responsabilità di quanto dichiarato e descritto nel D.P.S. è di totale responsabilità del titolare del trattamento, è quindi auspicabile che la raccolta delle informazioni, l'analisi dei rischi, delle problematiche, delle procedure, ecc… sia redatta in stretta collaborazione tra fornitore esterno e persone interne che si assumeranno la titolarità, le responsabilità e gli incarichi relativamente al trattamento dei dati personali. In tal modo le persone interessate avranno coscienza del proprio ruolo e le conoscenze sufficienti per mantenere un livello minimo di sicurezza atto ad evitare alti rischi per l'azienda stessa.

Un'osservazione: data la varietà e la complessità del problema della sicurezza dei dati nei sistemi informatici, la normativa non può prevedere e definire nel dettaglio le caratteristiche di un sistema intrinsecamente sicuro. Possiamo definire un sistema ben progettato quello che garantirà un buon livello di sicurezza relativamente all'importanza e all'appetibilità dei dati che dovrà gestire. Il grado di sicurezza non sarà nemmeno costante nel tempo ma dipenderà da nuovi virus, nuovi sistemi di intrusione nelle reti o dalla scoperta di falle nella sicurezza dei programmi e dei sistemi operativi utilizzati. Dipenderà anche dall'adozione di nuovi strumenti di difesa o dallo sviluppo di quelli in essere.
Quindi sia le problematiche relative alla sicurezza che tutte le attività previste nel D.P.S. saranno soprattutto dettate dal buon senso, evitando oneri eccessivi che non siano commisurati alle effettive necessità, ma evitando anche comportamenti "insani" come scrivere la password di rete sul post-it incollato sul monitor.

1.2 MISURE MINIME

Coloro che trattano i dati mediante strumenti elettronici, rispondono al titolo V del Codice che disciplina la sicurezza dei dati e dei sistemi. In particolare, in relazione alle misure di sicurezza, il Codice stabilisce che i dati personali oggetto di trattamento debbono essere custoditi e controllati anche in relazione alle conoscenze acquisiti in base al progresso tecniche nonché alla natura dei dati ed alle specifiche caratteristiche del trattamento al fine di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i

rischi di distruzione o perdita dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta. Vige pertanto un obbligo di adozione di misure minime di sicurezza.

Ma cosa si intende con questa espressione? È il Codice stesso che ci risponde, definendo misure minime quell'insieme di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che individuano il livello minimo di protezione richiesto dalla normativa rispetto ai rischi sopraelencati.
In pratica, il Codice identifica tali misure in un elenco preciso, secondo cui il trattamento dei dati personali effettuato con strumenti elettronici è subordinato all'adozione di specifiche misure.

- Occorre predisporre l'utilizzazione di un sistema di autenticazione informatica, ovvero il trattamento dei dati personali deve essere consentito solo agli incaricati muniti di credenziali di autenticazione, cioè di un codice per l'identificazione dell'incaricato associato ad una parola chiave (login/password) riservata e conosciuta esclusivamente dall'incaricato stesso, sul quale grava l'obbligo di adozione delle cautele necessarie al fine di assicurare la segretezza della componente riservata della credenziale, nonché l'obbligo di custodire diligentemente i dispositivi in suo possesso ed uso esclusivo.
- Il legislatore stabilisce un minimo di otto caratteri per quanto riguarda la parola chiave (salvo il caso in cui lo strumento elettronico non lo consenta).
- Altra misura di sicurezza è identificata nell'obbligo di modifica della parola chiave almeno ogni sei mesi. Nel caso di il trattamento con strumenti elettronici abbia ad oggetto dati sensibili o giudiziari, la modifica deve essere effettuata ogni tre mesi.
- Altro obbligo imposto sta nel fatto che le login/password non utilizzate da almeno sei mesi debbano essere disattivate, derogando solo nell'ipotesi di un utilizzo unicamente finalizzato alla gestione tecnica, per cui non è richiesta tale scadenza di modifica.
- La verifica dei profili di autorizzazione deve avvenire almeno annualmente.
- C'è inoltre l'obbligo di redazione del documento programmatico entro il 31 marzo di ogni anno (nel 2005 la scadenza è prorogata al 31 dicembre).
- Il titolare di un trattamento di dati personali effettuato con strumenti elettronici, (e di dati sensibili o dati giudiziari sia in formato cartaceo che elettronico) deve redigere tale documento sulla sicurezza. Nel disciplinare tecnico allegato al Codice, sono stabiliti i passaggi essenziali mediante cui stendere il documento (appendice: Guida Operativa).
  - Innanzi tutto occorre individuare l'elenco dei trattamenti di dati personali al quale deve affiancarsi l'elenco inerente la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dati.
  - Segue pertanto, coerentemente allo scopo del documento programmatico, l'analisi che il titolare del trattamento deve fare in relazione ai rischi che incombono sui dati, indicando conseguentemente anche le misure che sono adottate al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali in relazione alla loro custodia ed accessibilità.
  - Vige l'obbligo di individuare anche le modalità che possono essere poste a favore del ripristino della disponibilità dei dati qualora si verifichino episodi di distruzione o danneggiamento (è il caso di ricordare che per il trattamento di dati sensibili o giudiziari occorre garantire il ripristino dell'accesso entro 7 giorni). Infine, gli incaricati del trattamento debbono essere resi edotti dei rischi che incombono sui dati mediante interventi formativi.
  - Qualora si verifichi l'ipotesi di trattamenti di dati personali affidati all'esterno della struttura, sul titolare grava l'obbligo di descrivere nel documento, i criteri adottati per garantire la sussistenza delle misure minime di sicurezza per quei dati.
- Possiamo dunque concludere che il nuovo Codice apporterà reali garanzie per la tutela dei dati personali, pur lasciando qualche perplessità in relazione agli oneri che molti titolari dei trattamenti dovranno sostenere al fine di adempiere alle normative.

Nota: In appendice si trovano alcuni utili schemi riassuntivi per la preparazione delle informazioni necessarie alla stesura del D.P.S. stesso.

2 SCOPO DEL D.P.S.

Il Documento Programmatico Sulla Sicurezza è adottato, ai sensi dell'art. 6 del D.P.R. n.318/1999 e del D.l.g.196/2003, per definire le politiche di sicurezza in materia di trattamento di dati personali, ed i criteri organizzativi per la loro attuazione.
In particolare nel Documento Programmatico Sulla Sicurezza vengono definiti i ruoli dei responsabili

- Titolare del Trattamento
- Responsabile del Trattamento
- Amministratore di Sistema
- Incaricato al Trattamento

e vengono inoltre definiti i criteri tecnici ed organizzativi per:

- la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
- i criteri e le procedure per assicurare l'integrità dei dati;
- i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per l'accesso tramite via telematica;
- i criteri per la prevenzione e la difesa da eventi dannosi casuali o dolosi delle informazioni (Disaster Recovery) e il relativo piano di ripristino (business continuity plan);
- l'elaborazione di un piano di formazione del personale per rendere consapevoli gli incaricati del Trattamento dei rischi individuati e dei modi per prevenire i danni.

3 PRINCIPI GENERALI

Le persone preposte, nell'ambito della propria organizzazione, opereranno in modo da:

- minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati personali
- minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali
- minimizzare la probabilità che i trattamenti dei dati personali siano modificati senza autorizzazione.

4 CAMPO DI APPLICAZIONE

4.1 TIPOLOGIE DI TRATTAMENTI

Il Documento Programmatico Sulla Sicurezza, unitamente al Regolamento Aziendale per l'utilizzo delle attrezzature informatiche, definisce le politiche e gli standard di sicurezza in merito al Trattamento dei dati personali.
Il Documento Programmatico Sulla Sicurezza riguarda tutti i dati personali:

- Comuni
- Sensibili
- Giudiziari

Il Documento Programmatico Sulla Sicurezza si applica al Trattamento di tutti i dati personali per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (esempio: cartacei, audio, visivi e audiovisivi, ecc.)

Il Documento Programmatico Sulla Sicurezza deve essere conosciuto ed applicato da:

- tutti i dipendenti
- tutti i collaboratori esterni
- tutte le persone che a qualsiasi titolo agiscono sui sistemi informativi (tecnici della manutenzione)

4.2 RIFERIMENTI NORMATIVI

- L.n. 675/1996;
- D.Lgs.n. 123/1997
- D.Lgs.n. 255/1997
- D.Lgs.n. 135/1998
- D.Lgs.n. 171/1998
- D.Lgs.n. 389/1998
- D.Lgs.n. 51/1999
- D.Lgs.n. 135/1999
- D.Lgs.n. 281/1999
- D.Lgs.n. 282/1999
- D.P.R.n. 318/1999
- L.n. 325 del 3/11/2000
- D.Lgs.n. 196/2003 del 30/06/2003
- Delibera 31 Marzo 2004
- Delibera 23 Aprile 2004 (tolto obbligo notifica per chi compila 770 per otto per mille)

5 FIGURE PREVISTE DALLA NORMATIVA

5.1 ELENCO DELLE FIGURE PREVISTE

I. **Titolare del trattamento:** il Titolare del trattamento deve individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi dell'art. 15, commi 1 e 2, della legge 675/1996. Il Titolare del trattamento affida al/ai Responsabile/i del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto.

II. **Responsabile del trattamento:** incarico assunto dal Titolare stesso o assunto con nomina del Titolare. I compiti possono essere diversi a seconda delle funzioni svolte. Il Responsabile del trattamento, nel proprio ambito, ha l'onere di individuare, nominare ed indicare per iscritto uno o più Incaricati del trattamento. Il Responsabile del trattamento dei dati ha il compito di collaborare con l'amministratore di sistema per salvaguardare operativamente i dati personali da distruzione, prelievo non autorizzato, utilizzo non consentito, e deve Informare il Titolare nella eventualità che si siano rilevati dei rischi.

III. **Incaricati del trattamento:** nominati dai Responsabili del trattamento, sono i soggetti che operano a vario titolo sui dati personali. Devono essere accuratamente formati sulle corrette procedure di trattamento e sui rischi potenziali. Devono eseguire i compiti a loro assegnati e segnalare ai Responsabili eventuali malfunzionamenti o divergenze del sistema dal funzionamento previsto.

IV. **Custode delle password:** figura facoltativa, spesso assunta dall'Amministratore di Sistema o dai Responsabili del trattamento. Se l'Amministratore ha pieni diritti di accesso a tutto il sistema, la sua password è l'unica da salvare e conservare in busta chiusa e in luogo protetto accessibile solo dal Titolare o dal Responsabile.

V. **Amministratore di Sistema:** prendere tutti i provvedimenti operativi necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di backup, correttamente conservate, verificare gli accessi sia degli incaricati che di altri non autorizzati.

VI. **Responsabile dei Backup:** figura facoltativa, spesso assunta dall'Amministratore di Sistema o dal Responsabile del Trattamento. Deve assicurarsi che le procedure di backup inizino e si concludano correttamente, che siano riposti correttamente e che sia possibile il recupero dei dati salvati.

5.2 TITOLARE DEL TRATTAMENTO

Tra i compiti che la Legge assegna al Titolare e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza. Quindi deve:

- proporre le procedure per la sicurezza dei dati e verificarne le necessità di aggiornamento
- predisporre l'amministrazione della sicurezza informatica dell'intero sistema
- effettuare periodici controlli e verifiche in merito al rispetto delle prescrizioni contenute nell'ultimo D.P.S. redatto (validità annuale)
- valutare periodicamente il livello di rischio di sicurezza dei dati.

Il Titolare del Trattamento ha il compito di verificare che vengano attivate tutte le misure tali da garantire che i dati personali siano:

- trattati in modo lecito e secondo modalità corrette.
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del Trattamento in termini compatibili con tali scopi.
- esatti e, se necessario, aggiornati.
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati.
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Il Titolare del Trattamento è tenuto a nominare ed incaricare per iscritto uno o più Responsabili del Trattamento dei dati, ai quali è delegato il compito di verificare che vengano correttamente adottate le misure di sicurezza ai sensi dell'art. 28 del Dlg.196/2003.

- La nomina del Responsabile del Trattamento non è un esonero di responsabilità. La responsabilità sia civile che penale del Trattamento resta a carico del Titolare.
- I Responsabili del Trattamento sono nominati per iscritto dal Titolare del Trattamento.
- Il Titolare del Trattamento deve anche pianificare annualmente il piano di formazione dei Responsabili del Trattamento.

Nota: normalmente i responsabili del Trattamento vengono nominate tra le persone interne all'organizzazione, nulla comunque vieta di nominare responsabili del Trattamento anche figure esterne ovviamente figure di cui il Titolare del Trattamento ha la massima fiducia.

5.3 RESPONSABILE DEL TRATTAMENTO

La nomina dei Responsabili del Trattamento dei dati, fatta per iscritto dal Titolare del Trattamento, è a tempo indeterminato.
La figura del Responsabile del Trattamento può anche coincidere con quella del Titolare del Trattamento qualora questi abbia le capacità tecniche necessarie.
Il Responsabile del Trattamento deve a sua volta identificare e nominare per iscritto uno o più persone incaricate del Trattamento dei dati. Queste non sono altro che le persone che hanno accesso ai dati per il loro lavoro.

Ai Responsabili del Trattamento deve essere consegnata obbligatoriamente copia di:

- Lettera di Incarico
- Regolamenti che riguardano la sicurezza

Il Responsabile del Trattamento dei dati ha il compito di:

- Mantenere un elenco delle persone Incaricate al Trattamento
- Collaborare con l'Amministratore (o gli Amministratori) di Sistema per mantenere l'elenco degli utenti dei sistemi verificando che le eventuali variazioni revoche di utenze, vengano periodicamente eseguite.
- Verificare che vengano rispettate le procedure per l'accesso ai locali controllati

(esempio locali CED chiusi a chiave, archivi chiusi a chiave ecc.)
- Verificare, in collaborazione con l'Amministratore di Sistema, il funzionamento dei programmi anti-virus, anti-spam, anti-spyware, ecc...
- Verificare, in collaborazione con l'Amministratore di Sistema, l'effettuazione corretta delle operazioni di sicurezza (backup, attivazione firewall, distruzione supporti non più usati, mantenimento corretto delle password, ecc…)
- Informare il Titolare del Trattamento sulle mancate corrispondenze con le norme di sicurezza e su eventuali incidenti
- Informare tempestivamente il Titolare nell'eventualità che si presentino anomalie di qualsiasi genere.
- Pianificare annualmente e promuovere lo svolgimento di un continuo programma di addestramento degli Incaricati del Trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza.
- Promuovere e garantire l'esecuzione del programma di audit (strutture medio grandi).

5.4 INCARICATI DEL TRATTAMENTO

Il Responsabile del Trattamento (o i Responsabili qualora ne siano nominati più di uno) devono a loro volta nominare gli incaricati del Trattamento ovvero nominare, sempre per iscritto, le persone che devono accedere ai dati per lo svolgimento delle loro funzioni.

- Il Responsabile del Trattamento inoltre deve vigilare e verificare che i singoli incaricati si comportino secondo quanto prescritto e si attengano alle misure di sicurezza adottate.
- I singoli incaricati del Trattamento sono nominati per iscritto dai Responsabili del Trattamento.
- La nomina deve essere fatta con una lettera di incarico in cui sono specificati i compiti assegnati.
- La nomina è a tempo indeterminato e può essere revocata in qualsiasi momento.

Il Responsabile del Trattamento deve affidare agli incaricati:

- Lettera di incarico
- "User-Id" personale per accesso ai sistemi. Le "User-Id", sempre personali, possono anche essere più di una nel caso di varie tipologie di sistemi informativi.
- Istruzioni relative ai criteri di sicurezza adottati
- Istruzioni inerenti i tipi di trattamenti leciti sui dati
- Istruzioni riguardanti la finalità del Trattamento

Gli Incaricati del Trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

- Svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel D.P.S. e le direttive del Responsabile
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del Trattamento
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali
- informare il Responsabile in caso di incidente di sicurezza che coinvolga dati personali.

Nota: nella nomina degli incaricati è possibile definire dei gruppi di persone che presentano la stessa caratteristica dei dati (esempio personale di segreteria, contabilità). In questo caso ci sono lo stesso le singole nomine individuali ma la descrizione dei tipi di dati cui le persone hanno accesso è fatta per funzioni ovvero per gruppi di appartenenza.

5.5 AMMINISTRATORE DI SISTEMA

Il Titolare del Trattamento dati o il Responsabile del Trattamento devono nominare uno o più amministratori di sistema a seconda delle aree di loro competenza.

- La nomina degli Amministratori di sistema deve essere fatta con lettera di incarico.
- La figura dell'amministratore di sistema può anche coincidere con quella del Responsabile del Trattamento qualora questo abbia le capacità tecniche necessarie.
- Il Titolare del Trattamento è tenuto a distribuire ai Responsabili del Trattamento l'elenco degli Amministratori di sistema autorizzati ed a mantenere aggiornato l'elenco segnalando tempestivamente eventuali revoche degli Amministratori di Sistema.

Agli amministratori di sistema deve essere obbligatoriamente consegnata:

- Lettera di Incarico
- Regolamenti che riguardano la sicurezza
- Dettaglio della tipologia di dati che vengono gestiti con il sistema informativo e la finalità del Trattamento.
- Indicazioni sul livello di sicurezza che si desidera dal sistema

Gli amministratori di sistema devono garantire il corretto funzionamento dei sistemi informativi ed in particolare devono verificare che tutte le procedure riguardanti le normative tecniche sulla tutela dei dati personali siano rispettate.

- Gestire la creazione e la revoca delle utenze sul sistema informativo assegnando ad ogni utente la propria "User-Id" che deve essere protetta con password e deve essere strettamente personale.
- Occuparsi della sicurezza dell'intero sistema informativo
- Effettuare periodicamente i backup per evitare perdite di dati
- Assicurarsi della corretta conservazione delle copie di backup

6 PIANO DI FORMAZIONE

6.1 SICUREZZA E ERRORI UMANI

La sicurezza di un sistema richiede innanzi tutto che le persone che ne fruiscono siano adeguatamente formate in merito agli strumenti che utilizzano ed alle finalità del loro lavoro.
Gli errori umani sono spesso una delle cause principali di perdite o danneggiamenti di dati e di involontario utilizzo degli stessi.
Il Titolare del Trattamento, in collaborazione con il Responsabile del Trattamento, deve quindi prevedere un piano di Formazione annuale per le persone.

6.2 PIANO DI FORMAZIONE DEGLI INCARICATI

Al Responsabile del Trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le necessità di formazione del personale incaricato al Trattamento dei dati.

Tipologie principali di formazione possono essere:

- Formazione relativa alla gestione logica dei dati
- Formazione specifica sui rischi cui si è esposti
- Formazione volta al corretto utilizzo degli strumenti tecnici

Gli incaricati non devono sapere quale operazione effettuare al verificarsi di un problema, ma dovrebbero essere in grado di capire l'eventuale gravità del problema per poter contattare il proprio Responsabile e/o l'amministratore del sistema fornendo loro una descrizione (circostanziata) del problema stesso.

Deve essere sempre data la massima importanza alle finalità del Trattamento in modo che le persone siano consce delle operazioni lecite con i dati in loro possesso e che abbiano ben chiaro quali possono essere dei trattamenti illeciti per prevenire dei trattamenti illeciti (esempio cessione ad altri soggetti di elenchi anagrafici) involontari dovuti solo ad ignoranza delle regole.
Analogamente deve essere previsto il piano di formazione anche per le persone responsabili dei backup e dei sistemi. Eventuali modifiche a software installato (nuove versioni, nuovi programmi ecc.) possono cambiare la tipologia di dati da salvare quindi il Responsabile dei backup deve essere messo al corrente di qualsiasi tipo di modifica sul sistema.
Per ogni incaricato del Trattamento il Responsabile del Trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata, utilizzando apposito modulo che deve essere trasmesso in copia controllata al Titolare del Trattamento.

7 OUT-SOURCING

7.1 RESPONSABILITÀ

Il fatto di affidare alcuni o tutti i servizi in Out-Sourcing (affidamento all'esterno a fornitori di servizi) non esonera il Titolare del Trattamento sulla vigilanza delle misure di sicurezza prese.
E' sempre il Titolare del Trattamento in prima persona che rischia se si è appoggiato ad una società poco seria o inadeguata che utilizza i dati fornitegli anche per altre finalità non incluse nel Trattamento.
Risulta, quindi, necessario ottenere dai fornitori di questi servizi delle garanzie sul corretto Trattamento dei dati personali affidatati loro, garanzie riportate in appositi documenti o direttamente sul contratto di fornitura.

7.2 CRITERI PER LA SCELTA DEGLI ENTI TERZI (OUT-SOURCING)

Il Titolare del trattamento può nominare Responsabile del trattamento in out-sourcing (o Amministratori di sistema a seconda dei casi) quei soggetti terzi che abbiano i requisiti individuati all'art.29 del DLG 129/2003 (che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza).
Il Trattamento dati in Out-Sourcing deve essere autorizzato esplicitamente per iscritto.
Nel caso di Out-Sourcing relativo al Trattamento dei dati è necessario dettagliare il luogo in cui avviene il Trattamento ed i soggetti interessati.

7.3 RESPONSABILE DEL TRATTAMENTO DEI DATI IN OUT-SOURCING

Per ogni trattamento affidato ad un soggetto esterno viene nominato un Responsabile del trattamento in out-sourcing, il Titolare del trattamento deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.
Il Titolare del Trattamento quando nomina il Responsabile del Trattamento dati in Out-Sourcing deve fornirgli obbligatoriamente:

- Lettera di Incarico
- Regolamenti che riguardano la sicurezza
- Modalità e finalità del Trattamento autorizzato

Il Responsabile del trattamento dei dati in out-sourcing deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dalla normativa.
Il Titolare del trattamento deve informare il Responsabile del trattamento dei dati in out-sourcing dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore. Il Responsabile del trattamento dei dati in out-sourcing deve accettare la nomina, utilizzando apposito modulo. La nomina del Responsabile del trattamento dei dati in out-sourcing deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

8 DATI OGGETTO DEL TRATTAMENTO

8.1 TIPOLOGIE

Un sistema informativo aziendale, secondo il tipo di attività e le dimensioni dell'azienda stessa, avrà registrato dati di varia natura. Tutte queste informazioni potranno appartenere a una o più delle seguenti macro-categorie:

- Dati in forma anonima (statistici)
- Dati personali generici (indirizzo, partita IVA…)
- Dati personali sensibili (dati sanitari, preferenze sessuali, politiche, religiose…)
- Dati personali giudiziari
- Dati di natura commerciale (fatturazione, vendite)
- Dati di natura tecnica (progetti, relazioni, disegni)

Il confine tra le varie tipologie di dati è abbastanza labile: una registrazione video che ritrae un gruppo di persone non è un dato sensibile ma se quelle persone fossero riprese a una festa religiosa o a una festa di un partito politico dal documento sarebbe possibile risalire al credo religioso o alle idee politiche quindi il dato diventa assimilabile ai dati sensibili. Lo stato di salute di una persona può essere desunta non solo dalla cartella clinica, ma anche dalla lista dei farmaci che assume.
Il Responsabile del Trattamento dei dati ha il compito di mantenere un elenco aggiornato delle tipologie dei dati trattati, unitamente all'elenco delle eventuali sedi in cui sono conservati.

8.2 Art.13 – INFORMATIVA

L'articolo 13 del dlg.196/2003 prevede che si debba dare un informativa alle persone in cui viene dettagliato il tipo di Trattamento di dati, la modalità di raccolta e la finalità stessa della raccolta.
Nella normale gestione commerciale non è previsto un obbligo di informativa per la raccolta dei dati inerenti la stretta gestione del rapporto commerciale ma questo riguarda solo la raccolta dei soli dati inerenti lo svolgimento della transazione commerciale (esempio consegna materiale, emissione di bolla e di fattura).
Qualora si cerchi comunque di organizzarsi una base dati in cui si segna qualche informazione personale in più, (esempio tipo di preferenze per un invito a pranzo, tipo di preferenze per un regalo, ecc.) si esula dalla stretta raccolta dati per lo svolgimento del rapporto commerciale quindi sarebbe opportuno dare l'informativa per la raccolta dati e richiedere il consenso controfirmato per accettazione. A maggior ragione se i dati trattati vengono anche forniti all'esterno per eventuali elaborazioni in Out-Sourcing.
In ogni caso, nel dubbio, la consegna di un'informativa alla persona mette al riparo da qualsiasi eventuale contestazione successiva.

8.3 Art.23 – CONSENSO

L'articolo 23 del dlg.196/2003 prevede che, qualora sia necessario raccogliere il consenso, questo debba essere espresso per iscritto. Non è valido un consenso espresso oralmente. Se vi è la necessità di chiedere il consenso ai proprietari dei dati personali, per il loro Trattamento, questi consensi controfirmati per accettazione devono essere archiviati e

catalogati in modo di essere in grado di esibirli in fase ispettiva.
Gli eventuali consensi scritti raccolti ai sensi della precedente normativa sulla privacy sono considerati nulli dalla nuova Normativa.
Qualora ci sia realmente la necessità di richiedere il consenso per il Trattamento dei dati, questo andrà nuovamente richiesto ai sensi del dlg.196/2003.
È importante specificare nell'informativa e quindi raccogliere la firma per le due principali tipologie di destinazione dei dati personali raccolti: dati mantenuti presso la propria azienda (a fini contrattuali, di lavoro, ecc…) e/o dati ceduti a terzi per gestioni in out-sourcing (es.: società di leasing, gestioni esterne varie, ecc…).

9 SISTEMA INFORMATIVO

9.1 DEFINIZIONE

Come già detto nell'introduzione con il termine sistema informativo si sottintende l'insieme di tutte le informazioni patrimonio dell'azienda in qualsiasi forma esse siano quindi si intendono sia i dati memorizzati in formato elettronico sui dischi dei calcolatori, che i tradizionali documenti cartacei o di altra natura tipo registrazioni audio, video o microfilm.
Per quanto riguarda la parte informatica, il Responsabile del Trattamento dei dati, in collaborazione con l'Amministratore di sistema, se è diverso dallo stesso, deve mantenere un inventario dei sistemi di elaborazione che costituiscono il sistema informativo su cui viene effettuato il Trattamento dei dati.

9.2 SERVER

Non è solo un PC "speciale", ma si tratta dell'insieme:

Computer (server)
dischi contenenti gli archivi (interni o separati)
sistemi di salvataggio (backup)
apparecchiature per la connessione di rete (switch, router …)
firewall (se di tipo hardware)

Deve essere situato in un luogo protetto (sala server o armadi speciali certificati) e tutelato da ogni danno possibile. Nel caso di piccole strutture si può considerare un luogo sicuro anche l'ufficio del Titolare del trattamento o dell'Amministratore di rete a patto che, in sua assenza, non sia accessibile da altri soggetti non autorizzati.

9.3 STAZIONE DI LAVORO

Per ogni sistema di elaborazione (computer, client, workstation) devono essere descritte le caratteristiche principali specificando se si tratta di un sistema:

- Non accessibile da altri elaboratori (stand-alone)
- In rete non accessibile al pubblico (lan, intranet, wan)
- In rete accessibile al pubblico (internet, bbs)

Per ogni sistema deve essere specificato il nome dell'Amministratore e l'elenco degli utenti Incaricati che lo utilizzano.
Per l'inventario dei sistemi di elaborazione deve essere utilizzato apposito modulo che deve essere conservato a cura del Responsabile del Trattamento dei dati in luogo sicuro.
Eccezioni: sistemi isolati (non in rete) che non contengono dati personali.

9.4 SUPPORTI DI MEMORIZZAZIONE

Sono considerati supporti di memorizzazione i dischi rigidi rimovibili, i nastri magnetici, le cassette (cartridge, DAT), i dischi magnetici o ottici rimovibili, i CD-ROM che contengono informazioni personali. I supporti contenenti dati sensibili devono, se possibile, essere

marcati con un'opportuna etichetta recante la dicitura: **"Contiene dati personali sensibili secondo la legge 675/96. Rispettare quanto previsto dal Trattamento"**.
I supporti devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in un armadio / cassetto chiuso a chiave.

9.5 INFORMAZIONI RESIDUE

Sono definite informazioni residue quei dati personali ancora leggibili dopo la cessazione di un Trattamento (es. nastri, o dischi magnetici, dischi ottici, ecc…).
I dati personali devono essere resi illeggibili quando non sia più necessario conservarli per gli scopi per cui sono stati raccolti e trattati.

9.6 STAMPANTI E FAX

Il controllo dei documenti stampati è responsabilità degli incaricati al Trattamento. La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

9.7 INTEGRITA' DEGLI ARCHIVI CARTACEI

Il Responsabile del Trattamento deve prendere le opportune precauzioni in modo di garantire l'integrità degli archivi cartacei contenenti dati personali.
A seconda della tipologia dei documenti devono essere dettagliate le modalità di archiviazione indicando il luogo idoneo all'archiviazione e le norme da rispettare per minimizzare il rischio di incendio o allagamento che potrebbe causare danneggiamenti all'archivio.
È necessario anche garantire la distruzione fisica dei documenti che non siano più utili o siano giunti a fine validità e verificare la distruzione anche di eventuali stampe temporanee.

9.8 INTEGRITA' DEI DATI SUI SISTEMI ELETTRONICI

Il Responsabile del Trattamento deve garantire l'integrità dei dati memorizzati sui sistemi informativi con il supporto degli Amministratori di sistema. Allo scopo deve essere redatto un documento in cui vengono analizzate le tecnologie utilizzate e viene definito un livello di rischio accettabile. Nel documento vengono definite le procedure di backup. In particolare per ogni sistema deve essere redatto un documento dettagliato in cui vengono definite:

- La tecnologia adottata per effettuare le copie di backup
- La politica di mantenimento delle copie storiche di backup
- La metodologia usata per effettuare le copie di backup (automatizzate o lanciate manualmente dall'operatore)
- Le modalità di controllo delle copie di backup
- L'addetto ad effettuare le copie di backup
- Le istruzioni e i comandi necessari per effettuare le copie di backup

Il documento deve essere redatto in apposito modulo e conservato a cura del Responsabile del Trattamento dei dati in luogo sicuro e deve essere trasmesso in copia controllata a:

- Amministratore di sistema di competenza
- Incaricati del Trattamento di competenza

9.9 PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati è necessario proteggere i sistemi contro i virus informatici e gli attacchi dall'esterno.
Il Responsabile del Trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.
Il Responsabile del Trattamento dei dati stabilisce inoltre la periodicità, (almeno ogni sei mesi richiesto dalla Legge), con cui debbono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza dei sistemi informativi.
In particolare, per ogni sistema debbono essere definite le seguenti specifiche:

- Il tipo di programma antivirus utilizzato
- La periodicità di aggiornamenti
- La modalità di verifica del corretto funzionamento del programma antivirus

Deve inoltre essere predisposto un modulo su cui annotare gli eventi relativi ai Virus informatici registrando la tipologia di virus trovati, la data di infezione e, se si riesce a determinarla, la fonte dell'infezione.
I moduli compilati ed aggiornati debbono essere conservati a cura del Responsabile del Trattamento dei dati in luogo sicuro.

9.10 INFEZIONI E CONTAGIO DA VIRUS INFORMATICI

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da virus informatici l'Amministratore di sistema deve provvedere a:

- Isolare il sistema
- Verificare se ci sono altri sistemi e supporti infettati con lo stesso virus informatico
- Identificare la procedura o il programma anti-virus adatto e bonificare il sistema infetto
- Ripetere le operazioni di verifica (ed eventuale bonifica) su tutti gli altri sistemi e supporti che ne sono sprovvisti

L'amministratore di sistema deve inoltre compilare apposito modulo di "Segnalazione dei contagi da virus informatici".
I moduli compilati devono essere conservati a cura del Responsabile del Trattamento dei dati in luogo sicuro.

9.11 CUSTODIA E CONSERVAZIONE DEI SUPPORTI DI BACKUP

L'Amministratore di sistema è Responsabile della custodia e della conservazione di supporti utilizzati per il backup dei dati. Per ogni banca dati deve essere indicato il luogo di

conservazione ed i supporti utilizzati per il backup dei dati.
Il luogo di conservazione deve essere individuato in modo che sia protetto da:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni ed atti vandalici
- Furto
- Incendio
- Allagamento

Una soluzione molto utilizzata è: mantenere in sede il backup giornaliero (a rotazione su 5/6 supporti, uno per ogni giorno della settimana) e mettere al sicuro in una cassetta di sicurezza il backup settimanale più recente.

9.12 ELIMINAZIONE O RIUTILIZZO DEI SUPPORTI DI BACKUP

Nel caso in cui, per motivi tecnologici, i dispositivi utilizzati per il backup non siano più riutilizzabili (cancellando il contenuto) i dispositivi che non serve più conservare (ad esempio CD-R obsoleti), devono essere distrutti rendendone illeggibile il contenuto a cura del Responsabile incaricato per i backup.
E' tassativamente vietato smaltire dispositivi di memorizzazione contenenti dati di backup senza averli preventivamente cancellati in modo sicuro o distrutti e cioè senza avere preventivamente resi inutilizzabili. Si ricorda che esistono strumenti che sono in grado di recuperare le informazioni da supporti che siano stati cancellati o formattati, quindi il miglior grado di sicurezza è la distruzione fisica del supporto.
La stessa avvertenza è valida anche per l'eliminazione di tabulati.
Nel caso di dispositivi riutilizzabili si deve provvedere ad una completa cancellazione del supporto prima di riutilizzarli nuovamente per i backup. Nel caso di un backup a nastro si tratta ad esempio di formattare preventivamente i nastri.

9.13 DISASTER RECOVERY E BUSINESS CONTINUITY PLAN

A seguito del progressivo sviluppo di strutture informatiche e telematiche nelle aziende sono apparsi evidenti i rischi connessi ad una possibile perdita di dati essenziali per la continuità del lavoro, ciò ha determinato la necessità di definire procedure esaustive per ovviare a tali eventualità. Tale fenomeno è denominato "Disaster Recovery", la cui piena comprensione è collegata al concetto complementare di piano di continuità del business ('Business Continuity Plan') che rappresenta l'esigenza di garantire la continuità della connessione tra tutte le funzioni del sistema informatico aziendale, attraverso la definizione di modelli tecnologici e organizzativi capaci di reagire ai malfunzionamenti e integrare le stesse infrastrutture di connessione. Con "Disaster Recovery" si intendono, invece, quelle iniziative tese alla salvaguardia dei processi interni a fronte di eventi eccezionali, che si traducono principalmente nell'esigenza di conservazione dei dati, ma anche nella possibilità di fruizione degli stessi in tempi ragionevoli.

È necessario sottolineare che l'espressione "Disaster Recovery" non va limitata ai soli pericoli connessi agli eventi naturali e catastrofici, perché la semplice interruzione delle linee di telecomunicazione o il guasto di qualche server critico (dovuto a guasto o errore umano) può bloccare l'operatività aziendale. In termini statistici la perdita dei dati avviene soprattutto per guasto dei componenti hardware e dei programmi software o per errore umano, mentre solo

in minima parte tale perdita dipende da disastri naturali o da introduzione di virus.

L'elemento chiave del "Disaster Recovery" è quindi il backup periodico delle informazioni. Backup che deve essere organizzato correttamente con un'attenta selezione delle informazioni da salvare. Non tutti i dati aziendali devono essere necessariamente salvati. Il piano di backup deve essere creato in collaborazione tra l'area aziendale relativa alla gestione dei sistemi informatici e le diverse divisioni dell'azienda. Le operazioni di Backup non devono intralciare il normale svolgimento del lavoro, non devono sottrarre troppe risorse per non interferire con le prestazioni della rete aziendale, devono poter salvare documenti aperti e database in uso.

Altre problematiche inerenti alle procedure di backup sono:

I. il tipo di procedura da eseguire per i salvataggi periodici (es: un backup completo ogni settimana ed uno incrementale giornaliero)
II. il riutilizzo dei supporti (nastri, dischi…)
III. la conservazione dei supporti
IV. la collocazione materiale del backup
    a. la conservazione interna all'azienda (che non offre sufficienti garanzie)
    b. la collocazione esterna presso un operatore specializzato
    c. la collocazione esterna presso un'altra sede
V. i tempi di recupero (restore) dell'informazione salvata (più lunghi per la collocazione esterna)

Il piano di "Disaster Recovery" è finalizzato al semplice ripristino delle principali funzioni operative essenziali e non al totale recupero del sistema, ma non è il semplice salvataggio e recupero dei dati. Il "Disaster Recovery" riguarda il recupero completo della piena funzionalità delle procedure che utilizzano i dati aziendali salvati. Traducendo: non mi serve avere salvato programmi e dati di fatturazione se poi non posso operare attivamente sulle fatture (fatte e nuove) in tempi brevi. Il "Disaster Recovery" e il Business Continuità Plan devono includere i tempi di reazione del sistema alla perdita di un server, alla interruzione di un cavo di rete, ecc…

9.14 CONTRATTI DI DISASTER RECOVERY

Come molti altri servizi accessori al proprio core business, anche quelli legati al "Disaster Recovery" possono essere affidati in Out-Sourcing a fornitori che oltre alla conservazione dei backup, possono assicurare la disponibilità di hardware e software già predisposto per l'immediata ripresa del lavoro.
Appare ovvio che in questi casi, nell'organizzare tutti gli aspetti, come quelli della sicurezza dei dati, azienda e fornitore sono inevitabilmente costrette a scambiarsi informazioni confidenziali relative alle procedure ed agli aspetti gestionali sviluppati (know-how, informazioni sui clienti, strumenti e software utilizzati, metodologie e sistemi, licenze, ecc…)
Quindi risulta necessario, sin dall'inizio, un accordo di riservatezza, che disciplini le fasi di ottenimento delle informazioni, le trattative e la redazione degli accordi contrattuali.
Alla stesura definitiva del contratto verranno precisate le garanzie sulla riservatezza complessiva relativa a tutte le informazioni comunicate da una parte all'altra sia prima che dopo la firma del contratto stesso.

10 MISURE DI SICUREZZA ADOTTATE

10.1 NORME GENERALI DI PREVENZIONE

In considerazione di quanto disposto dal D.P.R. 318/1999 e dal DLG 196/2003, è fatto divieto a chiunque di:

- Utilizzare qualsiasi supporto di memorizzazione (o stampa) diverso da quelli ufficiali.
- Cedere a terzi supporti contenenti dati soggetti al Trattamento se non Preventivamente autorizzate dal Responsabile.
- Effettuare copie personali su dispositivi rimovibili di qualsiasi natura (CD, Floppy, Dischi fissi, chiavi USB, Smartcard ecc.) di dati soggetti al Trattamento se non preventivamente autorizzare dal Responsabile del Trattamento.
- Effettuare trasmissioni telematiche (email, fax ecc) di dati soggetti al Trattamento se non Preventivamente autorizzate dal Responsabile.
- Portare in altro luogo fotocopie o stampe di elenchi, rubriche o dati di qualsiasi altra natura se non si è preventivamente autorizzati dal Responsabile del Trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del Trattamento dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del Trattamento.
- Fornire a terzi, non esplicitamente autorizzati per iscritto dal Responsabile del Trattamento, dei dati sotto forma di stampe, tabulati, elenchi, rubriche, archivi in qualsiasi formato riguardante i dati oggetto del Trattamento.

11 CONTROLLO ACCESSO

11.1 CONTROLLO ACCESSO AI LOCALI CONTENENTI ARCHIVI CARTACEI

Il Responsabile del Trattamento è tenuto a compilare e mantenere aggiornato, l'elenco degli uffici in cui sono archiviati i dati soggetti a Trattamento e compilare e tenere aggiornato l'elenco degli Incaricati che possono accedere a tali locali.
Qualora si tratti di dati Sensibili l'accesso agli eventuali archivi cartacei deve essere controllato e limitato alle sole persone autorizzate ad accedere a quei particolari dati.
Eventuali archivi cartacei contenenti dati Sensibili devono quindi essere mantenuti in idonei armadi o locali chiusi a chiave.
Il Responsabile del Trattamento ha il compito di definire le modalità di accesso a tali locali o armadi.

11.2 AREE AD ACCESSO CONTROLLATO

Sono definite aree ad accesso controllato quei locali che contengono apparecchiature informatiche critiche come definite nel paragrafo seguente, e archivi informatici contenenti dati personali.

- Devono essere all'interno di aree sotto la responsabilità dell'Azienda.
- Deve essere chiaramente identificato un "Responsabile dell'area".
- Il locale deve essere chiuso anche se presidiato, le chiavi sono custodite a cura del "Responsabile dell'area".
- L'accesso deve essere consentito solo alle persone autorizzate.
- L'accesso deve essere possibile solo dall'interno dell'area sotto la responsabilità dell'Azienda, eventuali uscite di sicurezza devono essere allarmate.

11.3 APPARECCHIATURE INFORMATICHE CRITICHE AI FINI DELLA SICUREZZA

Sono considerate apparecchiature informatiche critiche ai fini della sicurezza le seguenti apparecchiature se parte del Trattamento di dati personali:

- Computer, sia server che client (workstation), con la sola esclusione delle workstation ad uso esclusivamente personale non contenenti dati personali
- Unità a dischi ottici o magnetici e unità nastri (DAT, DLT, ecc.)
- Sistemi per la gestione delle LAN, switch, router, hub, ecc…

Le chiavi dei sistemi e delle apparecchiature non devono essere lasciate nelle serrature o nelle vicinanze.
Le apparecchiature di rete che non sono situate nelle aree ad accesso controllato, devono essere riposte almeno all'interno di armadi chiusi.

11.4 REGOLE DI GESTIONE

Il "Responsabile dell'area" ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità.

- Deve esserci una lista delle persone autorizzate ad accedere.
- La lista deve essere periodicamente controllata.
- I visitatori occasionali devono essere accompagnati.
- Gli ingressi fuori orario devono essere controllati.
- Deve essere assicurata l'esecuzione di periodici test sull'efficacia degli allarmi.

11.5 CONTROLLO ACCESSO ALLA SALA MACCHINE

L'accesso alla sala macchine (CED: locale dove risiedono i server) deve essere limitato ai soli utenti che hanno necessità di fare manutenzione sui sistemi, tipicamente gli amministratori di sistema.
Eventuale personale esterno, esempio tecnici dell'assistenza alle macchine, possono accedere alla sala macchine solo se accompagnati da uno degli Amministratori di sistema.
E' fatto divieto ai tecnici dell'assistenza di sostituire e portare in altra sede, parti di hardware su cui possono essere memorizzati dati soggetti a Trattamento (vedi dischi fissi).
Per un'eventuale sostituzione di disco fisso, prima di ritirare il vecchio disco fisso sostituito ci si deve accertare di avere preventivamente rimosso tutti i dati in esso contenuti (wiping).

11.6 SICUREZZA LOGICA

È tutto ciò che disciplina i diversi aspetti del controllo dell'accesso logico alle informazioni personali. Sono regolamentati gli accessi ai computer alle LAN, alla rete e alle banche dati del Sistema Informatico Aziendale.

Funzione Identificazione ed Autenticazione degli utenti: Tale funzione assicura che ad ogni potenziale utente dei sistemi o delle banche dati sia associato un identificativo (user-id). Quando un utente accede al sistema, alla banca dati o alla rete ne viene verificata l'identità mediante un successivo livello di controllo (es. password).

11.7 PROCEDURE PER L'ASSEGNAZIONE DELLE "User-Id"

Le utenze ("Login" o "User-Id") per l'accesso ai sistemi informativi vengono create dagli Amministratori di sistema in base ad apposito elenco con le autorizzazioni, predisposto dal Responsabile del Trattamento dei dati.
Per ogni "User-Id" deve essere assegnata la visibilità ai soli dati di sua competenza.
Non sono ammesse "User-Id" di gruppo, con la sola eccezione per i sistemi operativi della vecchia generazione (DOS, WINDOWS 3.x, WINDOWS 9X) che non prevedono una gestione multi-utente. In qualsiasi caso eventuali macchine dotate di vecchi sistemi operativi non possono essere utilizzate come archiviazione di dati soggetti a Trattamento ed in particolare modo di quei dati definiti Sensibili.
L'Amministratore di sistema provvede a revocare la "User-Id" degli eventuali utenti dimessi o degli utenti che, per una qualunque ragione, non devono più avere accesso al sistema.

Definizioni:

1. User-id: L'accesso ai sistemi, alle banche dati contenenti informazioni personali, o alla rete deve essere basata sulle effettive necessità del Trattamento. L'user-id deve poter

essere riconducibile ad un singolo individuo. L'utilizzo di user-id che non siano personali è normalmente vietato; potrà essere accettato dal Responsabile del Trattamento per casi particolari, ad esempio per applicazioni che permettono la sola lettura delle informazioni.

2. Assegnazione e revoca delle user-id ed abilitazioni: L'azienda gestisce la procedura per l'assegnazione delle user-id che permettono l'accesso ai sistemi, alle banche dati e alla rete del Sistema Informatico Aziendale. Quando un utente non ha più la necessità di accedere ad una banca dati o lascia l'azienda, il Responsabile dell'utente interessato chiederà all'Amministratore di sistema di disabilitare l'utenza non più necessaria. Non è consentito il riutilizzo di una user-id personale già assegnata ad altro utente.

11.8 PROCEDURE DI ASSEGNAZIONE DELLE PASSWORD

L'Amministratore di sistema deve mettere in grado gli utenti di essere autonomi nella gestione delle loro password. Devono quindi essere documentate le varie procedure necessarie per il cambio della password. La password degli utenti sono strettamente personali e non devono essere assegnate dall'amministratore di Sistema.
L'amministratore di sistema non è in grado di leggere una password di un utente ma, in qualsiasi momento, è in grado di azzerare o assegnare una nuova e diversa password all'utente. Questa nuova password dall'Amministratore di sistema deve essere immediatamente cambiata dal singolo utente.
L'unica eccezione alla gestione delle password, che devono essere strettamente personali, è fatta per le password amministrative dei sistemi (utente root, admin, administrator, sysdba ecc). Queste password sono uniche per il sistema e devono essere note a tutti gli Amministratori di quel particolare sistema. Queste password devono essere sostituite periodicamente e devono essere custodite in Cassaforte.

Definizioni:

1. Password: La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente. Le regole di seguito elencate sono vincolanti per tutti i sistemi e le workstation tramite le quali si può accedere alla rete e alle banche dati contenenti dati personali. Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc... devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo.

2. Regole d'oro per la creazione di password:
    a. La lunghezza minima della password è di 6 caratteri.
    b. Deve contenere almeno un carattere alfabetico ed uno numerico.
    c. Non deve contenere più di due caratteri identici consecutivi.
    d. Non deve essere simile alla password precedente.
    e. Non deve contenere l'user-id come parte della password.
    f. Deve essere cambiata almeno ogni 6 mesi.
    g. Non deve essere comunicata ad altri utenti.
    h. Non deve essere scritta nelle vicinanze della tastiera, del monitor o in modo facilmente identificabile.

3. Dove la tecnologia lo permette tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle.

4. Ripristino della password: Il ripristino della password deve essere fatta solo a fronte di una positiva identificazione del richiedente e dovrà essere cambiata subito dopo a cura del richiedente.

11.9 IDENTIFICAZIONE DEGLI ELABORATORI CONNESSI IN RETE PUBBLICA

All'Amministratore di sistema è affidato il compito di redigere e di aggiornare ad ogni variazione. L'Amministratore di sistema ha il compito di redigere un elenco dei sistemi visibili su rete pubblica (BBS, INTERNET ecc.) dettagliando le modalità di accesso e le procedure prese per difendere il contenuto dei sistemi.

11.10 CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il Responsabile del Trattamento dei dati stabilisce, con il supporto tecnico dell'Amministratore di sistema, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di Hacker su ogni Sistema collegato in rete pubblica.
I criteri debbono essere definiti dall'Amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- Le misure applicate per evitare intrusioni
- Le misure applicate per evitare contagi da virus informatici o da spyware

11.11 ACCESSO REMOTO E USO DEI MODEM

Le connessioni via modem tra i sistemi e la rete del Sistema Informatico Aziendale con reti e sistemi esterni possono rappresentare un serio rischio per il Sistema stesso. Come conseguenza di collegamenti non corretti dal punto di vista della sicurezza, è possibile che si esponga a rischio l'intero sistema informativo ed i dati in esso contenuti, ciò può avvenire senza che il dipendente se ne renda conto.
Per tale motivo ogni collegamento dall'interno verso l'esterno e viceversa deve rispettare i criteri di sicurezza qui esposti e quelli che verranno stabiliti dal Titolare e/o Responsabile.
Nel caso il collegamento sia di tipo TCP/IP tramite modem, non deve essere permesso il suo uso simultaneamente al collegamento interno.
Di norma i modem collegati alle workstation devono restare spenti se non utilizzati.

12 MISURE CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

12.1 PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Responsabile del Trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli Incaricati del Trattamento autorizzati al Trattamento dei dati personali.
In particolare, in caso di Trattamento automatizzato di dati, per ogni Incaricato del Trattamento deve essere indicato la "User-Id" assegnata.

12.2 VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DELLE AUTORIZZAZIONI

All'Amministratore di sistema è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le autorizzazioni di accesso ai dati oggetto del Trattamento e di aggiornare l'elenco degli utenti autorizzati utilizzando apposito modulo che deve essere conservato a cura del Responsabile del Trattamento dei dati in luogo sicuro e deve essere trasmesso in copia :

- Amministratore di sistema di competenza
- Custode della password di competenza

13 MANUTENZIONE DI APPARECCHIATURE E SISTEMI DI TRATTAMENTO DEI DATI

13.1 MANUTENZIONE DI SISTEMI DI ELABORAZIONE DEI DATI

All'Amministratore di sistema è affidato il compito di verificare ogni anno la situazione delle apparecchiature hardware installate con cui vengono trattati i dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche.
La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito tenendo conto anche dell'evoluzione tecnologica.

L'Amministratore di sistema deve compilare apposito modulo di evidenziazione dei rischi hardware" e darne segnalazione al Responsabile del Trattamento che, nel caso in cui esistano rischi evidenti deve segnalarlo al Titolare del Trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto Trattamento dei dati in conformità alle norme in vigore.

13.2 MANUTENZIONE DEI SISTEMI OPERATIVI

All'Amministratore di sistema, è affidato il compito di verificare ogni anno la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito

tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei Sistemi operativi installati
- Segnalazioni di Patch, Bug-Fix o Service-Pack per la rimozione di errori o malfunzionamenti
- Segnalazioni di Patch, Bug-Fix o Service-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di sistema deve compilare apposito modulo di "evidenziazione dei rischi sui Sistemi Operativi" e darne segnalazione al Responsabile del Trattamento che, nel caso in cui esistano rischi evidenti deve segnalarlo al Titolare del Trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto Trattamento dei dati in conformità alle norme in vigore.

13.3 MANUTENZIONE DELLE APPLICAZIONI SOFTWARE

All'Amministratore di sistema è affidato il compito di verificare ogni anno, la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità del software applicativo, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito.

tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.
L'Amministratore di sistema deve compilare apposito modulo di "Evidenziazione dei rischi nelle applicazioni" e darne segnalazione al Responsabile del Trattamento che, nel caso in cui esistano rischi evidenti deve segnalarlo al Titolare del Trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto Trattamento dei dati in conformità alle norme in vigore.

14 MISURE DI SALVAGUARDIA DEI DATI CARTACEI E AFFINI

14.1 NOMINA E ISTRUZIONI AGLI INCARICATI

Per quanto riguarda eventuali archivi non in formato elettronico ovvero archivi in formato cartaceo, microfilm, videocassette ecc. il Responsabile del Trattamento è tenuto a mantenere aggiornata la lista degli Incaricati autorizzati ad accedervi ed è tenuto ad emanare un regolamento che riporti le istruzioni per potere accedere a detti archivi.
I documenti prelevati dagli archivi per il Trattamento, devono essere obbligatoriamente riconsegnati alla fine del Trattamento stesso.
Qualora i documenti contengano dati sensibili e giudiziari (art. 22 e 24 L.675/96) gli incaricati sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.
L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari non è con sentito dopo l'orario di chiusura della normale attività.

14.2 COPIE DEGLI ATTI DEI DOCUMENTI

Quanto indicato nel punto precedente si applica anche a qualunque tipo di copia effettuata sui documenti contenenti dati personali.

15 PRIVACY E ORGANIZZAZIONE AZIENDALE

La tutela dei dati personali e la sua attuazione implica una serie di azioni che possono modificare sensibilmente i processi aziendali, richiede che si creino o si riorganizzino determinati flussi informativi e quindi ha forti implicazioni anche nelle procedure del manuale della qualità.
Le nuove norme di tutela della privacy si inseriscono in un quadro di certificazioni di più ampio respiro ad esempio:

- Sistema di Qualità ISO 9001
- Sistema Ambientale ISO 14000
- Sicurezza del posto di lavoro 626
- Nuove norme sulla tutele dei dati personali

Quelle che adesso sono solo le nuove norme sulla tutele dei dati personali possono domani inserirsi in una specie di certificazione, tipo la BS 7799 diventata ISO 17799, che è una certificazione di sicurezza per i sistemi informativi. Un sistema informativo sicuro è già un ottimo punto di partenza per un sistema informativo che tutela la riservatezza dei dati.

16 REVISIONI E APPLICABILITÀ

16.1 REVISIONI

Il D.P.S. , redatto nel mese di marzo di ogni anno, è valido per un anno. Entro tale termine deve essere oggetto di revisione per adeguarlo ad eventuali variazioni del livello di rischio a cui sono soggetti i dati personali e ad eventuali modifiche della tecnologia informatica e per meglio descrivere le modifiche apportate all'organizzazione aziendale.

Nel caso di modificazioni legislative e ulteriori chiarimenti del garante verrà valutato se il contenuto del documento è conforme ai requisiti della Legge, in caso contrario se ne dovrà curare un aggiornamento.

16.2 APPLICABILITÀ

1. Il Documento Programmatico sulla Sicurezza delle Informazioni si applica a tutta la struttura del Sistema Informatico Aziendale.
2. Il contenuto deve essere divulgato e spiegato a tutti gli incaricati.
3. La parte che riguarda i dipendenti deve essere divulgata e spiegata a cura dei diretti responsabili.
4. Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel D.P.S. dovranno essere rimosse nel più breve tempo possibile.

17 RESPONSABILITÀ CIVILE E PENALE

17.1 ASPETTI DI RESPONSABILITÀ PENALE

Così recita l'art. 169 del Testo Unico Privacy sull'omessa adozione di misure necessarie alla sicurezza dei dati:

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi.
3. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato.
4. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

17.2 ASPETTI DI RESPONSABILITÀ CIVILE

Il Testo Unico Privacy qualifica il Trattamento dei dati come attività pericolosa, art.2050 c.c.
È prevista pertanto una inversione dell'onere della prova nell'azione di risarcimento ex art.2043 c.c. - l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire la sicurezza dei dati detenuti.
A livello pratico questo significa che l'azienda, il professionista, la P.A. , ecc..., per evitare ogni responsabilità deve dimostrare di aver adottato "tutte le misure idonee ad evitare il danno", e quindi di aver messo in essere tutte le misure di sicurezza al meglio possibile (la miglior tecnologia disponibile).

In generale poi a carico dell'azienda risulta comunque la responsabilità ex art.2049 c.c. , ovvero la responsabilità prevista in capo a padroni e committenti.
L'art.2049 difatti recita: "padroni e committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze cui sono adibiti".

Crimini informatici commessi da dipendenti ed addebitabili all'azienda.

La legge 547/93 ha introdotto nel nostro ordinamento vari "crimini informatici", ovvero l'attentato a impianti informatici di pubblica utilità, falsificazione di documenti informatici, accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, violazione di corrispondenza telematica, intercettazione di e-mail, danneggiamento di sistemi informatici o telematici (...).

Il datore di lavoro rischia di essere ritenuto in concorso con il dipendente a lui subordinato che ha commesso il crimine informatico, per non aver posto in essere tutte le misure di prevenzione e controllo idonee a garantire la sicurezza del Trattamento dei dati.
La mancata adozione di tutte le misure idonee a ridurre al minimo i rischi viene considerata difatti un agevolazione alla commissione del crimine.

17.3 DANNI CAGIONATI ALL'INTERESSATO

Art.15 Danni cagionati per effetto del Trattamento

1. Chiunque cagiona danno ad altri per effetto del **Trattamento** di dati personali è tenuto al risarcimento ai sensi dell'art.2050 del codice civile.
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.
3. L'art.2050 c.c. parla di "attività pericolosa" ('elevata potenzialità di danno, per la natura dell'attività o dei mezzi di lavoro utilizzati). Il **Trattamento** dati viene dunque qualificato come esercizio di attività pericolosa.
4. Da questa qualificazione deriva un'importante conseguenza circa l'onere della prova. Solitamente chi si ritiene danneggiato da un fatto illecito, deve provare la responsabilità di colui che ha commesso il fatto. Nell'ipotesi regolata dall'art. 2050 è sancito invece il "principio dell'inversione dell'onere della prova". Sulla base di questo principio il danneggiato deve provare solo il fatto storico, mentre colui che effettua il **Trattamento**, e che quindi ha causato il fatto dannoso, a fini liberatori, deve dimostrare di aver adottato tutte le misure idonee ad evitarlo.
5. La prova è particolarmente rigorosa, in quanto non è sufficiente la sola dimostrazione, in negativo, di non aver commesso alcuna violazione della legge o delle regole di comune prudenza, ma è necessaria la prova positiva di aver impiegato ogni cura o misura atta ad impedire l'evento dannoso. NB: è risarcibile anche il danno non patrimoniale

Chi e' tenuto al risarcimento?

I soggetti tenuti al risarcimento dei danni causati dal Trattamento dei dati personali, sono il Titolare del Trattamento (ossia colui "cui competono le decisioni in ordine alle finalità del Trattamento" e "della sicurezza") ed il Responsabile del Trattamento (ossia colui che è preposto dal Titolare al Trattamento dei dati, avendo "esperienza, capacità ed affidabilità" tale da fornire "idonea garanzia del pieno rispetto delle disposizioni di legge in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza").

17.4 TABELLINA RIASSUNTIVA DELLE SANZIONI

ILLECITI CIVILI	SANZIONE
Art.161 Assenza informativa privacy per dati sensibili o giudiziari o in caso di trattamenti che presentano rischi specifici o di maggiore rilevanza del pregiudizio	Sanzione da 3.000 a 30.000 euro. (moltiplicabile per 3 a seconda delle condizioni economiche del contravventore.
Art.163 Omessa o incompleta notificazione al Garante	Sanzione da 10.000 a 60.000 euro.
Art.164 Omissione di fornire informazioni o esibire documenti richiesti dal Garante Privacy	Sanzione da 4.000 a 24.000 euro.
ILLECITI PENALI	SANZIONE
Art.167 Trattamento illecito di dati personali	Reclusione da 6 mesi a 3 anni. Possibile estinguere il reato ex art.169, pagando una somma di denaro se ci si regolarizza entro il termine prescritto (non + di 6 mesi)
Art.168 Falsità nelle dichiarazioni e notificazioni al Garante	Sanzione penale, reclusione da 6 mesi a 3 anni
Art.169 Omessa adozione di misure necessarie alla sicurezza dei dati	Arresto fino a 2 anni o sanzione amministrativa, pagamento di una somma da 10.000 a 50.000 euro.
Art.170 Inosservanza dei provvedimenti del Garante	Arresto da 3 mesi a 2 anni.

18 Appendice: IN SINTESI

18.1 I PASSI DA SEGUIRE

1. Occorre programmare un adeguamento alle attrezzature informatiche abbandonando quelle che non risultano più idonee per criteri di sicurezza o affidabilità alla gestione di dati personali.
2. Occorre un inventario degli archivi informatici contenenti dati personali (esempio programmi con gestione di anagrafiche e liste di indirizzi). Attenzione: non tutto quello che viene memorizzato sui dischi dei calcolatori è necessariamente un dato personale.
3. È necessario un inventario di tutte le misure di sicurezza prese. Misure fisiche come: allarmi, armadi, copie di sicurezza, antivirus ecc.. Misure logiche come: password, controllo accessi. Misure organizzative come: nomina delle varie figure richieste dalla Legge, invio Informative, raccolta di Consensi.
4. Si deve procedere alla redazione del documento riepilogativo, il D.P.S. (per le aziende che hanno già una struttura informatica definita e ben organizzata, la stesura del D.P.S. può essere l'occasione per riepilogare, riorganizzare, riordinare, ridefinire, ecc… procedure già in essere senza provocare troppi stravolgimenti)

ATTENZIONE: questa Legge interpreta la sicurezza come un fatto dinamico quindi, una volta attivate le misure minime e scritto il D.P.S. occorre mantenersi al passo verificando periodicamente l'attualità delle misure prese, il loro funzionamento e provvedendo all'aggiornamento periodico del D.P.S. con cadenza annuale. Solo le nomine hanno durata illimitata salvo revoca.

18.2 ESSENZA E VALIDITÀ DEL D.P.S.

- E' l'unico documento in grado di attestare l'adeguamento della struttura alla normativa sulla tutela dei dati personali essendo dotato di data certa.
- E' un documento che, se scritto bene, assume una certa complessità soprattutto per società di una certa dimensione con molte persone e con molti dati raccolti.
- Nel caso degli studi professionali o piccole imprese comunque la complessità del documento resta limitata data la tipologia molto specifica dell'attività.
- Deve descrivere la situazione attuale facendo un'analisi dei rischi, una distribuzione dei compiti, un esame delle misure approntate ed assegnando le responsabilità alle singole persone coinvolte.
- Il D.P.S. deve diventare il manuale di pianificazione della sicurezza dei dati in azienda:
- Deve descrivere come si tutelano i dati personali di dipendenti, collaboratori, clienti, utenti, fornitori ecc. in ogni fase e ad ogni livello (fisico, logico, organizzativo). In ogni caso si tratta di un consistente piano di gestione della sicurezza, disponibilità ed integrità dei dati, avente data certa a prova formale dell'adeguamento sostenuto.
- Ci sono vari modi per ottenere la data certa tra cui il più semplice può essere il timbro postale su TUTTE LE PAGINE.
- In alternativa è possibile presentare il documento e Giurarlo in Tribunale (in questo caso il costo dell'operazione sarà la sola marca da bollo e la data certa è quella del documento). L'integrità delle successive pagine è documentata mediante il timbro

di congiunzione che unisce tutti i fogli.

- Altra alternativa per avere la data certa è quella di firmare digitalmente il documento per chi ha a disposizione un dispositivo di firma digitale (lettore e smart card).
- Ci sono anche altre possibilità di firma digitale tramite programmi forniti da Camere di commercio o altre società certificate.
- Il D.P.S. , oltre ad avere data certa, deve essere aggiornato annualmente. Il testo unico impone come data per la redazione e l'aggiornamento il 31 marzo di ogni anno, solo per questo anno il termine è stato prorogato al 31 dicembre 2005.
- Una copia del D.P.S. deve essere custodita presso la sede per essere consultabile e deve essere esibita in caso di controlli.
- Il Titolare del Trattamento deve dare conto nella relazione accompagnatoria del bilancio aziendale annuale dell'avvenuta redazione / aggiornamento del D.P.S.
- Una documentazione in linea con la norma BS7779 e le linee guida ISO 17799:2000 permette di costruire e mantenere nel tempo i processi che determinano e definiscono ruoli, responsabilità e procedure conformi agli obiettivi del Sistema di Gestione per la Sicurezza delle Informazioni.

Molte dei documenti accessori richiesti dalla normativa (comunicazioni tra il Titolare, i Responsabili e l'Amministratore di sistema) nelle piccole realtà non sono necessari perché la stessa persona si incarica di più ruoli o possono essere brevi messaggi di posta elettronica (poi correttamente archiviati) o semplici tabelle con struttura prefissata allegate in posta.

19 Appendice: GUIDA OPERATIVA

(guida operativa tratta dal Sito del "garante per la protezione dei dati personali")

Guida operativa per redigere il Documento programmatico sulla sicurezza (D.P.S.) (Codice in materia di protezione dei dati personali art. 34 e Allegato B, regola 19, del d.lgs. 30 giugno 2003, n. 196)

19.1 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 D.P.S.

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 (v. tab. 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 scollegati da una rete locale, geografica o Internet; sistemi informativi più complessi).

Ulteriori elementi per descrivere gli strumenti (v. tab. 1.2) (Facoltativa) 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 (v. tab. 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 (v. tab. 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 / phishing 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 / organizzazione:
   - Accessi non autorizzati a locali/reparti ad accesso ristretto
   - Sottrazione di strumenti contenenti dati

- Eventi distruttivi naturali o artificiali (terremoti, fulmini, allagamenti, incendi, ecc.)
- Eventi distruttivi dolosi, accidentali o dovuti ad incuria
- Guasto ai 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 (v. tab. 4.2): (Facoltativo) 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 recupero 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 (v. tab. 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 (v. tab. 5.2): (Facoltativo). 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 affidata all'esterno: 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 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.

19.2 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 D.P.S..

Tabella 1.1 – Elenco dei trattamenti: informazioni essenziali
- Descrizione sintetica del Trattamento
- Natura dei dati trattati
- Finalità perseguita o attività svolta
- Categorie di interessati
- 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 (facoltativa)
- 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
- Struttura
- Trattamenti effettuati dalla struttura
- Descrizione dei compiti e delle responsabilità della struttura

Tabella 3 - Analisi dei rischi
- Rischi
- Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)

Eventi relativi agli operatori:
- Sottrazione di credenziali di autenticazione
- Carenza di consapevolezza
- Disattenzione o incuria
- Comportamenti sleali o fraudolenti
- Errore materiale
- Comportamenti degli operatori
- Altri eventi

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 agli strumenti
- Altri eventi

Eventi relativi all'organizzazione:
- Accessi non autorizzati a locali/reparti ad accesso ristretto
- Sottrazione di strumenti contenenti dati
- Eventi distruttivi naturali o artificiali (terremoti, fulmini, allagamenti, incendi, ecc.)
- Eventi distruttivi dolosi, accidentali o dovuti ad incuria
- Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)
- Errori umani nella gestione della sicurezza fisica
- Altri eventi

Tab. 4.1 – Le misure di sicurezza adottate o da adottare
- Misure
- Descrizione dei rischi contrastati
- Trattamenti interessati
- Misura già in essere
- Misura da adottare (tempi)
- Struttura o persone addette all'adozione

Tab. 4.2 - Scheda descrittiva delle misure adottate (Facoltativa)
- Scheda n.
- Compilata da
- Data di compilazione
- Misura
- Descrizione sintetica

- Elementi descrittivi
- Data aggiornamento

Tab. 5.1 - Criteri e procedure per il ripristino della disponibilità dei dati
- Ripristino
- Banca dati / data base / archivio di dati
- Criteri e procedure per il salvataggio e il ripristino dei dati
- Pianificazione delle prove di ripristino

Tab. 5.2 - Criteri e procedure per il salvataggio dei dati (Facoltativa)
- Salvataggio
- Banca dati
- Criteri e procedure per il salvataggio
- Luogo di custodia delle copie
- Struttura o persona incaricata del salvataggio

Tab. 6 - Pianificazione degli interventi formativi previsti
- Descrizione sintetica degli interventi formativi
- Classi di incarico o tipologie di incaricati interessati
- Tempi previsti

Tab. 7 - Trattamenti affidati all'esterno
- Descrizione sintetica dell'attività affidata all'esterno
- Trattamenti di dati interessati
- Soggetto esterno
- Descrizione dei criteri e degli impegni assunti per l'adozione delle misure

Tab. 8 - Cifratura dei dati o separazione dei dati identificativi (solo per organismi sanitari ed esercenti professioni sanitarie)
- Tecnica adottata
- Trattamenti di dati
- Protezione scelta (Cifratura / Separazione)
- Descrizione
- Informazioni utili

20 Appendice: ADEGUAMENTO ORGANIZZATIVO

20.1 PREMESSA

Il personale che lavora in una realtà aziendale, per lavorare in modo coordinato e per il raggiungimento di uno scopo comune, ha bisogno di essere inquadrato in modo preciso nell'organizzazione e di operare secondo regole comuni. Quindi ne consegue l'importanza di definire la struttura organizzativa individuando e nominando ufficialmente i vari ruoli aziendali. Un ruolo aziendale non è rappresentato solo dalla persona incaricata a ricoprirlo, ma anche dai compiti e dalle responsabilità proprie dello stesso. E' quindi indispensabile che per ogni ruolo, o per ogni classe di ruoli, vi sia un regolamento scritto, formalizzato in manuali interni o integrato nella lettera d'incarico.

20.2  COSA FARE PER ADEGUARE LA PROPRIA AZIENDA 

Il Titolare deve:

- Definire la struttura organizzativa.
- Nominare formalmente con una lettera d'incarico le varie figure;
- Definire le procedure interne che regolano i compiti di ogni figura; la scelta della gerarchia migliore dipende dalle capacità delle persone coinvolte;
- E' importante precisare che la struttura non è necessariamente rigida, ma spetta al Titolare scegliere quella che più si addice alla sua realtà aziendale.

Nella maggior parte delle aziende si è soliti trovare più ruoli attribuiti ad una stessa persona: nei piccoli uffici è probabile che l'amministratore di sistema sia anche il responsabile della sicurezza informatica ed il custode delle password. La presenza di persone distinte per ogni ruolo è un'esigenza che fa capo principalmente ad aziende medio-grandi.

20.3  COSA FARE NELLO SPECIFICO

Definire la struttura organizzativa individuando e nominando con apposita lettera d'incarico delle figure. Figure esplicitamente nominate e definite nel D.Lgs. 196/2003 sono:

- **Il Garante**: l'autorità istituita dalla legge n. 675 del 31 dicembre 1996 che tutela la riservatezza dei dati personali.
- **L'Interessato**: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
- **Il Titolare**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- **Il Responsabile**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
- **L'Incaricato**: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Altre figure individuate per una corretta gestione della sicurezza:

- **L'Amministratore di sistema**: persona responsabile dell'amministrazione di determinati strumenti elettronici. Può essere l'incaricato responsabile della sua postazione o una persona alla quale compete l'amministrazione di più postazioni.
- **Il Responsabile della sicurezza informatica**: persona con conoscenze informatiche adeguate a garantire la sicurezza informatica in azienda. Prepara il piano di sicurezza aziendale scegliendo gli strumenti e le procedure più idonee di salvaguardia per gli strumenti informatici aziendali ed i dati contenuti o passanti per essi.
- **Il Manutentore di sistema**: persona che si occupa degli interventi tecnici hardware e software sugli strumenti elettronici. Ad esempio: installazione antivirus, sostituzione componenti hardware, configurazione della rete…
- **Il Custode delle password**: persona incaricata alla custodia delle parole chiave delle credenziali di autenticazione delle persone incaricate al trattamento dati.
- **L'Incaricato al controllo dei locali**: persona responsabile dell'accesso ai locali nei quali si effettuano i trattamenti.
- **Il Professionista esterno**: professionista esterno chiamato a prestare il suo servizio utilizzando i dati personali raccolti dall'azienda ed a lui affidati. (commercialista, fornitore di servizi,…).
- **L'Esterno che accede ai locali**: persona che per motivi ben definiti accede ai locali nei quali vengono trattati i dati personali (tecnico hardware o software, elettricista,…).

Ricordiamo che è possibile attribuire più ruoli ad una stessa persona, in questa circostanza si può predisporre una sola lettera d'incarico comprendente più ruoli identificati dalle competenze e dai compiti.
Per garantire la continuità dell'attività è bene che alcuni ruoli siano assegnati ad almeno due persone diverse o che si predispongano dei regolamenti interni grazie ai quali si possano attivare procedure idonee a sopperire alla momentanea mancanza di una figura.
È opportuno individuare un elenco di professionisti e fornitori esterni che possano intervenire al verificarsi di un evento che possa pregiudicare la continuità dell'attività aziendale e definire contrattualmente i tempi di attivazione dei suddetti.

L'elenco potrà essere organizzato in una tabella.

NOME	ATTIVITA'	TELEFONO	TEMPI	NOTE

Alle figure devono essere date precise indicazioni per l'espletamento della loro funzione lavorativa. Vi è quindi la necessità di predisporre dei manuali operativi nei quali siano indicati con precisione i compiti e le responsabilità proprie del ruolo.
Le procedure che il Titolare del trattamento deve regolamentare sono:

- accesso ai locali del trattamento;
- accesso agli archivi cartacei;
- utilizzo dei sistemi informatici;
- utilizzo di internet;
- utilizzo della posta elettronica;
- procedura di backup e ripristino;
- procedura per l'esercizio dei diritti degli interessati;
- piano di formazione.

21 Appendice: Elenco delle informazioni necessarie

1) Breve descrizione delle attività primarie, secondarie dell'azienda e delle attività accessorie. Elenco dei soggetti aventi collaborazioni in atto o future con comunione di informazioni contenenti dati personali (es.: paghe e stipendi gestito all'esterno).

2) Lista completa delle sedi operative (principali, secondarie, consociate…).

3) Elenco dei trattamenti di dati personali mediante:

a. individuazione dei dati personali trattati e relativi strumenti (gestione clienti, fornitori, utenti, posta elettronica, personale, fatturazione, ecc…)

   i. dati comuni relativi a clienti / utenti
   ii. dati comuni relativi a fornitori
   iii. dati comuni relativi ad altri soggetti
   iv. dati biometrici relativi a clienti / personale
   v. dati idonei a rilevare la posizione di persone / oggetti
   vi. dati relativi allo svolgimento di attività economica e/o commerciale
   vii. dati di natura giudiziaria
   viii. dati relativi al personale, candidati, (anche sensibili)
   ix. dati di natura anche sensibile relativi a clienti / utenti
   x. dati idonei a rilevare lo stato di salute

b. elenco, codifica e descrizione delle aree e dei locali interessati al Trattamento
c. elenco, codifica e descrizione degli strumenti con i quali si effettuano i trattamenti (server e client, pc, reti, sistemi operativi, programmi installati, ecc…) e loro collocazione all'interno dei locali stessi
d. elenco e catalogazione degli strumenti accessori e loro collocazione quali fax, stampanti, impianti di videosorveglianza, ecc…
e. elenco dei dati personali (comuni, sensibili e giudiziari) mantenuti su supporti cartacei (e comunque non elettronici), elenco e codifica dei luoghi della loro archiviazione, collocazione all'interno dei locali stessi, misure di protezione, modalità di accesso, valutazione sulla loro perdita / distruzione / furto

4) Organigramma del personale: distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al Trattamento dei dati:

a. Individuazione del Titolare del Trattamento dei dati
b. Individuazione dei responsabili del Trattamento dei dati - Lista dei responsabili di ogni ufficio / reparto / mansione
c. Individuazione degli incaricati al Trattamento dei dati - Lista del personale addetto per ogni ufficio / mansione
d. Individuazione dell'amministratore del sistema informativo.

5) Lista delle istruzioni specifiche fornite ai soggetti incaricati e in particolare:

a. procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di Trattamento che questo tipo di dati richiedono
b. modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi

c. modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia al preposto alla custodia della parola chiave
d. prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro
e. procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi
f. procedure per il salvataggio dei dati
g. modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali
h. aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

6) Analisi dei rischi a cui sono soggetti i dati (guasti, incendi, furti, incuria, ecc…). Analisi del danno relativo ai server e ai client e alla rete. L'analisi dei possibili rischi che gravano sui dati è da effettuare combinando due tipi di rilevazioni:

a. la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono
b. le caratteristiche degli strumenti utilizzati per il Trattamento dei dati.

Elenco dei possibili rischi da valutare per livello di gravità e grado di probabilità:

I. Rischio d'area legato all'accesso non autorizzato nei Locali (vandalismo, furto, sabotaggio…)
II. Rischio guasti tecnici hardware, software, supporti (rotture, virus…)
III. Rischio penetrazione nelle reti di comunicazione (hacking…)
IV. Rischio legato ad errori umani (impreparazione, incuria, dolo…)
V. Rischio d'area per possibili eventi distruttivi (incendi, crolli, black-out…)

7) Elenco delle misure già adottate e a budget per garantire la difesa dai rischi elencati:

a. protezione delle aree e dei locali ove si svolge il Trattamento dei dati personali
b. antifurti
c. porte blindate o controllate da Badge.
d. procedure per la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali
e. procedure di sicurezza logica e gestionale, nell'ambito degli strumenti elettronici
f. programmi anti-virus, anti-spam, anti-spyware ecc…
g. sistemi di backup
h. i firewall
i. gruppi di continuità dell'alimentazione elettrica
j. dispositivi antincendio previsti dalla normativa vigente
k. impianto di condizionamento

8) Criteri e modalità di ripristino dei dati a seguito di perdita per distruzione o danneggiamento. Stima dei tempi di recupero per tipologia di operazione.

9) Lista delle misure minime di sicurezza in caso di affidamento del Trattamento esterno dei dati personali. Lista dei fornitori di servizio e lista delle garanzie assicurate con apposito documento o per contratto.

10) Lista delle procedure per il controllo sullo stato della sicurezza, pianificazione delle verifiche di:

a. accesso fisico a locali dove si svolge il Trattamento
b. procedure di archiviazione e custodia dati trattati
c. efficacia e utilizzo misure di sicurezza strumenti elettronici
d. integrità dei dati e delle loro copie di backup
e. distruzione dei supporti magnetici non più riutilizzabili
f. livello di informazione degli interessati

11) Pianificazione dei programmi di formazione per il personale.

a. al momento dell'ingresso in servizio
b. in occasione di cambiamenti di mansione
c. in occasione dell'introduzioni di nuovi strumenti e programmi informatici

22 Appendice: MISURE MINIME

22.1 Allegato: Decreto del Presidente della Repubblica n. 318 del 28 luglio 1999

Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge n. 675 del 31 dicembre 1996

Preambolo

IL PRESIDENTE DELLA REPUBBLICA

Visto l'articolo 87, comma quinto, della Costituzione;
Visto l'articolo 15 della legge 31 dicembre 1996, n. 675, recante «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»;
Ritenuto che ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675, occorre individuare, in via preventiva, le misure minime di sicurezza per i dati personali oggetto di trattamento, al fine di assicurare il funzionamento delle misure sanzionatorie penali previste dall'articolo 36 della medesima legge;
Visto l'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400;
Sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante per la protezione dei dati personali;
Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 26 aprile 1999;
Ritenuto di dover comunque garantire la possibilità, in caso di più incaricati del trattamento, di limitare l'accesso a determinati dati personali attraverso la previsione di una specifica parola chiave per tali dati, senza operare, quindi, alcuna equiparazione tra tale ipotesi e quella relativa alla previsione di un'unica parola chiave per l'accesso al sistema;
Viste le deliberazioni del Consiglio dei Ministri, adottate nelle riunioni del 16 luglio e del 23 luglio 1999;
Sulla proposta del Ministro di grazia e giustizia;

EMANA

il seguente regolamento:

CAPO I - PRINCIPI GENERALI

Art.1- Definizioni

Ai fini del presente regolamento si applicano le definizioni elencate nell'articolo1 della legge 31 dicembre1996, n. 675, di seguito denominata legge. Ai medesimi fini si intendono per:

a. «misure minime»: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'articolo 15, comma 1, della legge;
b. «strumenti»:i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;
c. «amministratori di sistema»: i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

CAPO II - TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI - Sezione I -Trattamento dei dati personali effettuato mediante elaboratori non accessibili da altri elaboratori o terminali

Art.2 - Individuazione degli incaricati

1. Salvo quanto previsto dall'articolo 8, se il trattamento dei dati personali è effettuato per fini diversi da quelli di cui all'articolo 3 della legge mediante elaboratori non accessibili da altri elaboratori o terminali, devono essere adottate, anteriormente all'inizio del trattamento, le seguenti misure:

a. prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, consentirne l'autonoma sostituzione, previa comunicazione ai soggetti preposti ai sensi della lettera b);
b. individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime.

CAPO II - TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI - Sezione II - Trattamento dei dati personali effettuato mediante elaboratori accessibili in rete

Art.3 - Classificazione

1. Ai fini della presente sezione gli elaboratori accessibili in rete impiegati nel trattamento dei dati personali sono distinti in:

a. elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico;
b. elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico.

Art.4 - Codici identificativi e protezione degli elaboratori

1. Nel caso di trattamenti effettuati con gli elaboratori di cui all'articolo 3, oltre a quanto previsto dall'articolo 2 devono essere adottate le seguenti misure:

    a. a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse;
    b. i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
    c. gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.

2. Le disposizioni di cui al comma 1, lettere a) e b), non si applicano ai trattamenti dei dati personali di cui è consentita la diffusione.

Art.5 - Accesso ai dati particolari

1. Per il trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato ai sensi dell'articolo 3, l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Se il trattamento è effettuato ai sensi dell'articolo 3, comma 1, lettera b), sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico.
2. L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.

3. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.
4. L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
5. La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso.
6. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.
7. Le disposizioni di cui ai commi da la 6 non si applicano al trattamento dei dati personali di cui è consentita la diffusione.

Art.6 - Documento programmatico sulla sicurezza

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato mediante gli elaboratori indicati nell'articolo 3, comma l, lettera b), deve essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:

    a. i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
    b. i criteri e le procedure per assicurare l'integrità dei dati;
    c. i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
    d. l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

2. L'efficacia delle misure di sicurezza adottate ai sensi del comma 1 deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

Art.7. - Reimpiego dei supporti di memorizzazione

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato con gli strumenti di cui all'articolo 3, i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

CAPO II - TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI - Sezione III - Trattamento dei dati personali effettuato per fini esclusivamente personali

Art.8 - Parola chiave

1. Ai sensi dell'articolo 3 della legge, il trattamento per fini esclusivamente personali dei dati di cui agli articoli 22 e 24 della legge, effettuato con elaboratori stabilmente accessibili da altri elaboratori, è soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche di dati.

CAPO III - TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI

Art.9 - Trattamento di dati personali

1. Nel caso di trattamento di dati personali per fini diversi da quelli dell'articolo 3 della legge, effettuato, con strumenti diversi da quelli previsti dal capo II, sono osservate le seguenti modalità:
   a. nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli articoli 8, comma 5, e 19 della legge, il titolare o, se designato, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
   b. gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.

2. Nel caso di trattamento di dati di cui agli articoli 22 e 24 della legge, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalità:

a. se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura;
b. l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

Art.10 - Conservazione della documentazione relativa al trattamento

I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali di cui agli articoli 22 e 24 della legge devono essere conservati e custoditi con le modalità di cui all'articolo 9.
Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 28 luglio 1999

CIAMPI
D'Alema, Presidente del Consiglio dei Ministri
Diliberto, Ministro di grazia e giustizia
Visto, il Guardasigilli: Diliberto

23 Appendice: GLOSSARIO

AMMINISTRATORE DI SISTEMA: è il soggetto che si occupa del sistema informatico e delle risorse operative.

ANTI-SPAM: software atto a bloccare il fenomeno dello SPAMMING.

ANTI-SPYWARE: software che cerca e riconosce ed elimina il software detto SPYWARE.

ANTI-VIRUS: software specializzato a riconoscere, prevenire ed eliminare virus informatici.

BANCA DATI: (archivio o archivi relazionati) è una raccolta di dati che possono essere dati personali.

BUG-FIX: software di aggiornamento per la soluzione di un malfunzionamento di un programma già installato.

CARTRIDGE: tipo di cassetta per il backup dei dati.

CLIENT: stazione di lavoro collegata a un server tramite una rete.

DAT: tecnologia per il salvataggio dei dati. Si intende anche la cassetta che la utilizza.

DATI PERSONALI: sono tutte le informazioni relative a persona fisica (persona giuridica, ente od associazione) identificate o identificabili. Esempio: Nome, cognome, indirizzo, numeri telefonici, Numero di Patente, P. IVA.

DATI SENSIBILI: sono i dati che devono essere maggiormente tutelati, e sono relativi a razza etnia, ad eventuali adesioni a partiti (ritenute sindacali), organizzazioni a carattere religioso, politico, associazioni di categoria, nonché dati personali idonei a rilevare lo stato di salute (cartelle mediche) e la vita sessuale del singolo.

FIREWALL: è uno strumento hardware o software che può limitare l'accesso da rete interna (o da stazione di lavoro) a rete pubblica e viceversa.

INCARICATO: colui/coloro che elabora i dati personali sulla base delle istruzioni scritte del Titolare o del Responsabile.

INTERESSATO: persona fisica (la persona giuridica, l'ente o l'associazione) cui si riferiscono i dati personali trattati.

LAN: rete dati interna aziendale.

LOGIN: vedi USER ID.

LOGON: vedi USER ID.

MISURE DI SICUREZZA: sono misure atte a custodire i documenti approntando degli accorgimenti (armadietti chiusi a chiave, firewall (hardware o software che impedisce accessi indesiderati all'interno della struttura di una rete), wiping (cancellazione fisica dei dati da un supporto elettronico), accesso selezionato ai dati...)

PASSWORD: parola chiave, una sequenza di lettere e/o numeri, che serve per accordare l'accesso al sistema informatico agli utenti.

PATCH: aggiornamento per il miglioramento di un programma già installato.

RESPONSABILE DEL TRATTAMENTO DEI DATI: è la persona fisica (la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che il Titolare (che decide) prepone al Trattamento di dati personali. Titolare e Responsabile possono essere la stessa persona. I compiti affidatigli devono essere analiticamente specificati per iscritto.

ROUTER: apparecchio elettronico che può smistare informazioni tra server e client e tra varie reti.

SERVER: computer attrezzato per fornire servizi ad altri computer a lui collegati con una rete.

SERVICE-PACK: software di aggiornamento di un sistema operativo installato.

SPAMMING: tecnica di invio di messaggi di posta indesiderati al fine di disturbo, pubblicità o altro.

SPYWARE: software si installa in modo fraudolento in un computer e che tenta di raccogliere, senza autorizzazione, informazioni dal computer dove risiede per la successiva trasmissione degli stessi via rete pubblica.

TCP/IP: protocollo di trasmissione dati tipico di Internet.

TITOLARE DEL TRATTAMENTO: persona fisica, (la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che ha la competenza a decidere in ordine alle finalità, alle modalità del Trattamento di dati personali ed alla loro sicurezza.

TRATTAMENTO DEI DATI: consiste in qualunque operazione o insieme di operazioni, eseguite o meno grazie ad un computer, riguardanti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

USERNAME: vedi USER ID.

USER ID (USERNAME o LOGIN o LOGON): è un codice identificativo personale formato da lettere e/o numeri. Viene sempre abbinato alla password (segreta).

VIRUS: programma che si installa in modo fraudolento in un computer e che può provocare danni di varia natura al software e all'hardware del computer ospite.

WAN: rete geografica aziendale che utilizza cavi dedicati e riservati.

WIPING: tecnica di cancellazione definitiva dei dati dai supporti elettronici (HD, dischi, nastri…). Vengono scritte delle informazioni casuali al posto di quelle salvate.

WORKSTATION: singola stazione di lavoro (pc) generalmente collegata in rete.

24 NOTE

Autore:

Gabriele Cappelletti: Consulenze Informatiche Direzionali - Cappelletti.ict@Tiscali.it

Il presente documento è in continuo sviluppo e arricchimento: sono ben accetti eventuali suggerimenti, segnalazioni e commenti.