INDICE GENERALE

SCOPO....2
CAMPO DI APPLICAZIONE....3
RIFERIMENTI NORMATIVI....3
FIGURE PREVISTE DALLA NORMATIVA....4
TITOLARE DEL TRATTAMENTO....4
RESPONSABILE DEL TRATTAMENTO....5
INCARICATI DEL TRATTAMENTO....6
AMMINISTRATORE DI SISTEMA....7
OUT-SOURCING....8
TRATTAMENTO DEI DATI IN OUT-SOURCING....8
DATI OGGETTI DEL TRATTAMENTO....9
art 13 – INFORMATIVA....9
art. 23 – CONSENSO....10
SISTEMA INFORMATIVO....11
PROCEDURE PER GARANTIRE L'INTEGRITA' DEGLI ARCHIVI CARTACEI....11
PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI SUI SISTEMI ELETTRONICI....12
PROTEZIONE DA VIRUS INFORMATICI....13
INFEZIONI E CONTAGIO DA VIRUS INFORMATICI....13
CUSTODIA E CONSERVAZIONE DEI SUPPORTI DI BACKUP....14
ELIMINAZIONE O RIUTILIZZO DEI SUPPORTI DI BACKUP....14
PIANO DI FORMAZIONE....15
PIANO DI FORMAZIONE DEGLI INCARICATI....15
MISURE DI SICUREZZA ADOTTATE....16
NORME GENERALI DI PREVENZIONE....16
CONTROLLO ACCESSO....17
CONTROLLO ACCESSO AI LOCALI CONTENENTI ARCHIVI CARTACEI....17
CONTROLLO ACCESSO ALLA SALA MACCHINE....17
PROCEDURE PER L'ASSEGNAZIONE DEGLI USER-ID....18
PROCEDURE DI ASSEGNAZIONE DELLE PASSWORD....18
IDENTIFICAZIONE DEGLI ELABORATORI CONNESSI IN RETE PUBBLICA....19
CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DATI....19
MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO....20
PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI....20
VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO DELLE AUTORIZZAZIONI....20
MANUTENZIONE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI....21
MANUTENZIONE DI SISTEMI DI ELABORAZIONE DEI DATI....21
MANUTENZIONE DEI SISTEMI OPERATIVI....21
MANUTENZIONE DELLE APPLICAZIONI SOFTWARE....22
MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI....23
NOMINA E ISTRUZIONI AGLI INCARICATI....23
COPIE DEGLI ATTI DEI DOCUMENTI....23
Privacy ed ORGANIZZAZIONE AZIENDALE....24
REVISIONI....25
ALLEGATO INDICE ARTICOLI LEGGE....26

SCOPO

Il presente 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 le redazioni di accesso per via telematica;
- l'elaborazione di un piano di formazione al personale per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

CAMPO DI APPLICAZIONE

Il Documento Programmatico Sulla Sicurezza, in unione 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)

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
- Dlg. n. 196/2003 del 30/giu/2003
- Delibera 31 Marzo 2004
- Delibera 23 Aprile 2004 (tolto obbligo notifica per chi compila 770 per 8 %o

FIGURE PREVISTE DALLA NORMATIVA

TITOLARE DEL TRATTAMENTO

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.

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.

I Responsabili del trattamento sono nominati per iscritto dal Titolare del trattamento.

Il titolare del trattamento ha il compito di verificare che siano attivate tutte le misure tali da garantire che i dati personali sono:

- trattati in modo lecito e secondo correttezza.
- 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.
- Pianificare annualmente il piano di formazione dei Responsabili del trattamento.

RESPONSABILE DEL TRATTAMENTO

La nomina dei Responsabili del trattamento dei dati deve essere fatta per iscritto a cura del Titolare del trattamento ed 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.

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 o 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.
- Informare tempestivamente il Titolare nella eventualità che si presentino anomalie di qualsiasi genere.
- Pianificare Annualmente il piano di formazione per gli incaricati

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.

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.

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

Il Responsabile del trattamento deve dare 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 inerenti i criteri di sicurezza adottati
- Istruzioni inerenti i tipi di trattamenti leciti sui dati
- Istruzioni riguardanti la finalità del trattamento

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.

Agli Incaricati del trattamento deve essere obbligatoriamente fornito:

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

OUT-SOURCING

Il fatto di affidare alcuni o tutti i servizi in Out-Sourcing 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 che utilizza i dati forniteli anche per altre finalià non incluse nel trattamento.

TRATTAMENTO DEI DATI IN OUT-SOURCING

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in tutto o in parte a

soggetti terzi, in Out-Sourcing, nominandoli Responsabili del trattamento o Amministratori di sistema a seconda dei casi.

Nel caso di Out-Sourcing relativo al trattamento dei dati è necessario dettagliare il luogo in cui avviene il trattamento ed i soggetti interessati.

I soggetti terzi a cui affidate trattamenti dati in Out-Sourcing devono essere selezionati il base ai requisiti all'art.29 del DLG 129/2003 (che per esperienza, capacita' 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. Il Titolare del trattamento deve quindi nominare un Responsabile del trattamento dati in Out-Sourcing al quale deve essere obbligatoriamente fornita:

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

DATI OGGETTI DEL TRATTAMENTO

Un sistema informativo aziendale, indipendentemente dalle dimensioni dell'organizzazione, contiene dati di varia natura tutti comunque riconducibili alle seguenti macro-categorie:

- Dati in forma anonima
- Dati personali generici
- Dati personali sensibili
- 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 foto che ritrae un gruppo di persone non è un dato sensibile ma se quelle persone fossero ritratte alla festa di un partito politico dalla foto è possibile risalire alle idee politiche quindi il dato diventa sensibile.

Il Responsabile del trattamento dei dati ha il compito di mantenere aggiornato l'elenco delle tipologie dei dati trattati.

Qualora il trattamento dei dati avvenga in più sedi occorre anche un elenco di tutte le sedi in cui sono conservati i dati e la tipologia di dati conservati.

(Esempio: Studio tecnico, elenchi anagrafici clienti/fornitori conservati sia in studio che in cantiere)

art 13 – INFORMATIVA

L'articolo 13 del dlg 196 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.

art. 23 – CONSENSO

L'art. 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.

SISTEMA INFORMATIVO

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 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.

Per ogni sistema di elaborazione 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
- In rete accessibile al pubblico

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.

PROCEDURE PER GARANTIRE L'INTEGRITA' DEGLI ARCHIVI CARTACEI

Il Responsabile del trattamento deve prendere le opportune precauzioni in modo di garantire l'integrità degli archivi cartacei.

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.

PROCEDURE PER GARANTIRE L'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

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.

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 infettati con lo stesso virus informatico
- Identificare il programma anti virus adatto e bonificare il sistema infetto
- Installare il programma anti virus adatto su tutti gli altri sistemi 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.

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
- Allargamento

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.

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.

PIANO DI FORMAZIONE

La sicurezza di un sistema richiede innanzitutto 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 involontari 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.

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.

Deve essere sempre data la massima importanza alle finalità del trattamento in modo che le persone siano coscienti 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.

MISURE DI SICUREZZA ADOTTATE

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.
- 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.

CONTROLLO ACCESSO

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.

Per i dati in forma elettronica sono memorizzati solo sui server ed accessibili mediante la coppia USER-ID/password personale degli utenti.

CONTROLLO ACCESSO ALLA SALA MACCHINE

L'accesso alla sala macchine (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.

PROCEDURE PER L'ASSEGNAZIONE DEGLI USER-ID

Gli USER-ID per l'accesso ai sistemi informativi vengono creati dagli Amministratori di sistema in base ad apposito elenco con le autorizzazioni ,predisposto dal Responsabile del trattamento dei dati.

Le USER-ID sono strettamente personali degli utenti e devono essere protette con password mantenute segrete a cura degli stessi utenti.

Per ogni USER-ID deve essere assegnata la visibilità ai soli dati di sua competenza.

E' cura dell'utente proteggere la propria USER-ID con una password che deve essere tenuta strettamente personale.

Non sono ammesse USER-ID di di gruppo, con la sola eccezione per i sistemi operativi della vecchia generazione (DOS, WINDOWS 3.x, WINDOWS 9X) che non prevedono una gestione multiutente. 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.

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 riassegnare una diversa password all'utente. Questa password riassegnata 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.

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.

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

MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

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 lo USER-ID assegnato.

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

MANUTENZIONE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI

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.

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 utilizzati
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti
- Segnalazioni di Patch, Fix o System-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.

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.

MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI

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 consentito dopo l'orario di chiusura della normale attività.

COPIE DEGLI ATTI DEI DOCUMENTI

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

Privacy ed ORGANIZZAZIONE AZIENDALE

La messa a norma per quanto riguarda la tutele dei dati personali è una cosa che impatta sui processi aziendali, richiede che ci siano determinati flussi informativi e quindi finisce immancabilmente a rientrare 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.

REVISIONI

Il presente Documento Programmatico Sulla Sicurezza (DPSS), redatto nel mese di marzo 2004, verrà revisionato annualmente ed eventualmente sottoposto a modifiche.

ALLEGATO INDICE ARTICOLI LEGGE

CAPITOLI "Codice in materia di protezione dei dati personali"

PARTE I
DISPOSIZIONI GENERALI
- Titolo I
- PRINCIPI GENERALI
  - Art. 1 (Diritto alla protezione dei dati personali)
  - Art. 2 (Finalita)
  - Art. 3 (Principio di necessita' nel trattamento dei dati)
  - Art. 4 (Definizioni)
  - Art. 5 (Oggetto ed ambito di applicazione)
  - Art. 6 (Disciplina del trattamento)
- Titolo II
- DIRITTI DELL'INTERESSATO
  - Art. 7 (Diritto di accesso ai dati personali ed altri diritti)
  - Art. 8 (Esercizio dei diritti)
  - Art. 9 (Modalita' di esercizio)
  - Art. 10 (Riscontro all'interessato)
- Titolo III
- REGOLE GENERALI PER IL TRATTAMENTO DEI DATI
  - CAPO I REGOLE PER TUTTI I TRATTAMENTI
  - Art. 11 (Modalita' del trattamento e requisiti dei dati)
  - Art. 12 (Codici di deontologia e di buona condotta)
  - Art. 13 (Informativa)
  - Art. 14 (Definizione di profili e della personalita' dell'interessato)
  - Art. 15 (Danni cagionati per effetto del trattamento)
  - Art. 16 (Cessazione del trattamento)
  - Art. 17 (Trattamento che presenta rischi specifici)
- CAPO II
- REGOLE ULTERIORI PER I SOGGETTI PUBBLICI
  - Art. 18 (Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici)
  - Art. 19 (Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari)
  - Art. 20 (Principi applicabili al trattamento di dati sensibili)
  - Art. 21 (Principi applicabili al trattamento di dati giudiziari)
  - Art. 22 (Principi applicabili al trattamento di dati sensibili e giudiziari)
- CAPO III
- REGOLE ULTERIORI PER PRIVATI ED ENTI PUBBLICI ECONOMICI
  - Art. 23 (Consenso)
  - Art. 24 (Casi nei quali puo' essere effettuato il trattamento senza consenso)
  - Art. 25 (Divieti di comunicazione e diffusione)
  - Art. 26 (Garanzie per i dati sensibili)
  - Art. 27 (Garanzie per i dati giudiziari)
- TITOLO IV
- SOGGETTI CHE EFFETTUANO IL TRATTAMENTO
  - Art. 28 (Titolare del trattamento)
  - Art. 29 (Responsabile del trattamento)
  - Art. 30 (Incaricati del trattamento)
- Titolo V
- SICUREZZA DEI DATI E DEI SISTEMI
- CAPO I
- MISURE DI SICUREZZA
  - Art. 31 (Obblighi di sicurezza)
  - Art. 32 (Particolari titolari)
- CAPO II
- MISURE MINIME DI SICUREZZA
  - Art. 33 (Misure minime)
  - Art. 34 (Trattamenti con strumenti elettronici)
  - Art. 35 (Trattamenti senza l'ausilio di strumenti elettronici)
  - Art. 36 (Adeguamento)
- Titolo VI
- ADEMPIMENTI
  - Art. 37 (Notificazione del trattamento)
  - Art. 38 (Modalita' di notificazione)
  - Art. 39 (Obblighi di comunicazione)
  - Art. 40 (Autorizzazioni generali)
  - Art. 41 (Richieste di autorizzazione)
- TITOLO VII
- TRASFERIMENTO DEI DATI ALL'ESTERO
  - Art. 42 (Trasferimenti all'interno dell'Unione europea)
  - Art. 43 (Trasferimenti consentiti in Paesi terzi)
  - Art. 44 (Altri trasferimenti consentiti)
  - Art. 45 (Trasferimenti vietati)

PARTE II
DISPOSIZIONI RELATIVE A SPECIFICI SETTORI

TITOLO I
TRATTAMENTI IN AMBITO GIUDIZIARIO
CAPO I
PROFILI GENERALI
Art. 46 (Titolari dei trattamenti)
Art. 47 (Trattamenti per ragioni di giustizia)
Art. 48 (Banche di dati di uffici giudiziari)
Art. 49 (Disposizioni di attuazione)
CAPO II
MINORI
Art. 50 (Notizie o immagini relative a minori)
CAPO III
INFORMATICA GIURIDICA
Art. 51 (Principi generali)
Art. 52 (Dati identificativi degli interessati)
TITOLO II
TRATTAMENTI DA PARTE DI FORZE DI POLIZIA
CAPO I
PROFILI GENERALI
Art. 53 (Ambito applicativo e titolari dei trattamenti)
Art. 54 (Modalita' di trattamento e flussi di dati)
Art. 55 (Particolari tecnologie)
Art. 56 (Tutela dell'interessato)
Art. 57 (Disposizioni di attuazione)
TITOLO III
DIFESA E SICUREZZA DELLO STATO
CAPO I
PROFILI GENERALI
Art. 58 (Disposizioni applicabili)
TITOLO IV
TRATTAMENTI IN AMBITO PUBBLICO
CAPO I
ACCESSO A DOCUMENTI AMMINISTRATIVI
Art. 59 (Accesso a documenti amministrativi)
Art. 60 (Dati idonei a rivelare lo stato di salute e la vita sessuale)
CAPO II
REGISTRI PUBBLICI E ALBI PROFESSIONALI
Art. 61 (Utilizzazione di dati pubblici)
CAPO III
STATO CIVILE, ANAGRAFI E LISTE ELETTORALI
Art. 62 (Dati sensibili e giudiziari)
Art. 63 (Consultazione di atti)
CAPO IV
FINALITA' DI RILEVANTE INTERESSE PUBBLICO
Art. 64 (Cittadinanza, immigrazione e condizione dello straniero)
Art. 65 (Diritti politici e pubblicita' dell'attivita' di organi)
Art. 66 (Materia tributaria e doganale)
Art. 67 (Attivita' di controllo e ispettive)
Art. 68 (Benefici economici ed abilitazioni)
Art. 69 (Onorificenze, ricompense e riconoscimenti)
Art. 70 (Volontariato e obiezione di coscienza)
Art. 71 (Attivita' sanzionatorie e di tutela)
Art. 72 (Rapporti con enti di culto)
Art. 73 (Altre finalita' in ambito amministrativo e sociale)
CAPO V
PARTICOLARI CONTRASSEGNI
Art. 74 (Contrassegni su veicoli e accessi a centri storici)
TITOLO V
TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO
CAPO I
PRINCIPI GENERALI
Art. 75 (Ambito applicativo)
Art. 76 (Esercenti professioni sanitarie e organismi sanitari pubblici)
CAPO II
MODALITA' SEMPLIFICATE PER INFORMATIVA E CONSENSO
Art. 77 (Casi di semplificazione)
Art. 78 (Informativa del medico di medicina generale o del pediatra)
Art. 79 (Informativa da parte di organismi sanitari)
Art. 80 (Informativa da parte di altri soggetti pubblici)
Art. 81 (Prestazione del consenso)
Art. 82 (Emergenze e tutela della salute e dell'incolumita' fisica)
Art. 83 (Altre misure per il rispetto dei diritti degli interessati)
Art. 84 (Comunicazione di dati all'interessato)
CAPO III
FINALITA' DI RILEVANTE INTERESSE PUBBLICO
Art. 85 (Compiti del Servizio sanitario nazionale)
Art. 86 (Altre finalita' di rilevante interesse pubblico)

CAPO IV
PRESCRIZIONI MEDICHE
Art. 87 (Medicinali a carico del Servizio sanitario nazionale)
Art. 88 (Medicinali non a carico del Servizio sanitario nazionale)
Art. 89 (Casi particolari)
CAPO V
DATI GENETICI
Art. 90 (Trattamento dei dati genetici e donatori di midollo osseo)
CAPO VI
DISPOSIZIONI VARIE
Art. 91 (Dati trattati mediante carte)
Art. 92 (Cartelle cliniche)
Art. 93 (Certificato di assistenza al parto)
Art. 94 (Banche di dati, registri e schedari in ambito sanitario)
TITOLO VI
ISTRUZIONE
CAPO I
PROFILI GENERALI
Art. 95 (Dati sensibili e giudiziari)
Art. 96 (Trattamento di dati relativi a studenti)
TITOLO VII
TRATTAMENTO PER SCOPI STORICI, STATISTICI O SCIENTIFICI
CAPO I
PROFILI GENERALI
Art. 97 (Ambito applicativo)
Art. 98 (Finalita' di rilevante interesse pubblico)
Art. 99 (Compatibilita' tra scopi e durata del trattamento)
Art. 100 (Dati relativi ad attivita' di studio e ricerca)
CAPO II
TRATTAMENTO PER SCOPI STORICI
Art. 101 (Modalita' di trattamento)
Art. 102 (Codice di deontologia e di buona condotta)
Art. 103 (Consultazione di documenti conservati in archivi)
CAPO III
TRATTAMENTO PER SCOPI STATISTICI O SCIENTIFICI
Art. 104 (Ambito applicativo e dati identificativi per scopi statistici o scientifici)
Art. 105 (Modalita' di trattamento)
Art. 106 (Codici di deontologia e di buona condotta)
Art. 107 (Trattamento di dati sensibili)
Art. 108 (Sistema statistico nazionale)
Art. 109 (Dati statistici relativi all'evento della nascita)
Art. 110 (Ricerca medica, biomedica ed epidemiologica)
TITOLO VIII
LAVORO E PREVIDENZA SOCIALE
CAPO I
PROFILI GENERALI
Art. 111 (Codice di deontologia e di buona condotta)
Art. 112 (Finalita' di rilevante interesse pubblico)
CAPO II
ANNUNCI DI LAVORO E DATI RIGUARDANTI PRESTATORI DI LAVORO
Art. 113 (Raccolta di dati e pertinenza)
CAPO III
DIVIETO DI CONTROLLO A DISTANZA E TELELAVORO
Art. 114 (Controllo a distanza)
Art. 115 (Telelavoro e lavoro a domicilio)
CAPO IV
ISTITUTI DI PATRONATO E DI ASSISTENZA SOCIALE
Art. 116 (Conoscibilita' di dati su mandato dell'interessato)
TITOLO IX
SISTEMA BANCARIO, FINANZIARIO ED ASSICURATIVO
CAPO I
SISTEMI INFORMATIVI
Art. 117 (Affidabilita' e puntualita' nei pagamenti)
Art. 118 (Informazioni commerciali)
Art. 119 (Dati relativi al comportamento debitorio)
Art. 120 (Sinistri)
TITOLO X
COMUNICAZIONI ELETTRONICHE
CAPO I
SERVIZI DI COMUNICAZIONE ELETTRONICA
Art. 121 (Servizi interessati)
Art. 122 (Informazioni raccolte nei riguardi dell'abbonato o dell'utente)
Art. 123 (Dati relativi al traffico)
Art. 124 (Fatturazione dettagliata)
Art. 125 (Identificazione della linea)
Art. 126 (Dati relativi all'ubicazione)
Art. 127 (Chiamate di disturbo e di emergenza)

Art. 128 (Trasferimento automatico della chiamata)
Art. 129 (Elenchi di abbonati)
Art. 130 (Comunicazioni indesiderate)
Art. 131 (Informazioni ad abbonati e utenti)
Art. 132 (Conservazione di dati di traffico per altre finalita)
CAPO II
INTERNET E RETI TELEMATICHE
Art. 133 (Codice di deontologia e di buona condotta)
CAPO III
VIDEOSORVEGLIANZA
Art. 134 (Codice di deontologia e di buona condotta)
TITOLO XI
LIBERE PROFESSIONI E INVESTIGAZIONE PRIVATA
CAPO I
PROFILI GENERALI
Art. 135 (Codice di deontologia e di buona condotta)
TITOLO XII
GIORNALISMO ED ESPRESSIONE LETTERARIA ED ARTISTICA
CAPO I
PROFILI GENERALI
Art. 136 (Finalita' giornalistiche e altre manifestazioni del pensiero)
Art. 137 (Disposizioni applicabili)
Art. 138 (Segreto professionale)
CAPO II
CODICE DI DEONTOLOGIA
Art. 139 (Codice di deontologia relativo ad attivita' giornalistiche)
TITOLO XIII
MARKETING DIRETTO
CAPO I
PROFILI GENERALI
Art. 140 (Codice di deontologia e di buona condotta)
PARTE III
TUTELA DELL'INTERESSATO E SANZIONI
TITOLO I
TUTELA AMMINISTRATIVA E GIURISDIZIONALE
CAPO I
TUTELA DINANZI AL GARANTE
SEZIONE I
PRINCIPI GENERALI
Art. 141 (Forme di tutela)
SEZIONE II
TUTELA AMMINISTRATIVA
Art. 142 (Proposizione dei reclami)
Art. 143 (Procedimento per i reclami)
Art. 144 (Segnalazioni)
SEZIONE III
TUTELA ALTERNATIVA A QUELLA GIURISDIZIONALE
Art. 145 (Ricorsi)
Art. 146 (Interpello preventivo)
Art. 147 (Presentazione del ricorso)
Art. 148 (Inammissibilita' del ricorso)
Art. 149 (Procedimento relativo al ricorso)
Art. 150 (Provvedimenti a seguito del ricorso)
Art. 151 (Opposizione)
CAPO II
TUTELA GIURISDIZIONALE
Art. 152 (Autorita' giudiziaria ordinaria)
TITOLO II
L'AUTORITA'
CAPO I
IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
Art. 153 (Il Garante)
Art. 154 (Compiti)
CAPO II
L'UFFICIO DEL GARANTE
Art. 155 (Principi applicabili)
Art. 156 (Ruolo organico e personale)
CAPO III
ACCERTAMENTI E CONTROLLI
Art. 157 (Richiesta di informazioni e di esibizione di documenti)
Art. 158 (Accertamenti)
Art. 159 (Modalita)
Art. 160 (Particolari accertamenti)
TITOLO III
SANZIONI
CAPO I
VIOLAZIONI AMMINISTRATIVE

Art. 161 (Omessa o inidonea informativa all'interessato)
Art. 162 (Altre fattispecie)
Art. 163 (Omessa o incompleta notificazione)
Art. 164 (Omessa informazione o esibizione al Garante)
Art. 165 (Pubblicazione del provvedimento del Garante)
Art. 166 (Procedimento di applicazione)
CAPO II
ILLECITI PENALI
Art. 167 (Trattamento illecito di dati)
Art. 168 (Falsita' nelle dichiarazioni e notificazioni al Garante)
Art. 169 (Misure di sicurezza)
Art. 170 (Inosservanza di provvedimenti del Garante)
Art. 171 (Altre fattispecie)
Art. 172 (Pene accessorie)
TITOLO IV
DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI
CAPO I
DISPOSIZIONI DI MODIFICA
Art. 173 (Convenzione di applicazione dell'Accordo di Schengen)
Art. 174 (Notifiche di atti e vendite giudiziarie)
Art. 175 (Forze di polizia)
Art. 176 (Soggetti pubblici)
Art. 177 (Disciplina anagrafica, dello stato civile e delle liste elettorali)
Art. 178 (Disposizioni in materia sanitaria)
Art. 179 (Altre modifiche)
CAPO II
DISPOSIZIONI TRANSITORIE
Art. 180 (Misure di sicurezza)
Art. 181 (Altre disposizioni transitorie)
Art. 182 (Ufficio del Garante)
CAPO III
ABROGAZIONI
Art. 183 (Norme abrogate)
CAPO IV
NORME FINALI
Art. 184 (Attuazione di direttive europee)
Art. 185 (Allegazione dei codici di deontologia e di buona condotta)
Art. 186 (Entrata in vigore)
ALLEGATO A
ALLEGATO B
ALLEGATO C)