

*Nuove tecnologie, nuove responsabilità:
focus sul D.Lgs. 196/2003*

Daniela Rocca – daniela.rocca@sng.it

Politecnico di Milano, 4 giugno 2004

Privacy = diritto

- Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali
- Convenzione di Strasburgo n. 108/1981 del Consiglio d'Europa
- Carta dei diritti fondamentali dell'Unione Europea
- Direttiva 1995/46/CE; Direttiva 2002/58/CE

- ...il diritto di "essere lasciati soli"
- ...il diritto di controllare le informazioni che ci riguardano (Fidelity cards, TV digitale, Sms,...)

- TRE DIRITTI FONDAMENTALI DELLA PERSONA:
 - **diritto alla privacy**
 - **libera trasmissione e circolazione delle informazioni**
 - **bisogno di sicurezza**

EQUILIBRIO!

Privacy = Responsabilità

- La conoscenza degli aspetti legali correlati alla sicurezza informatica e' di fondamentale importanza per un'efficace gestione delle reti telematiche.
- Le nuove tecnologie hanno creato nuove responsabilità' per gli operatori e le Aziende ed hanno reso necessaria un'attenta analisi degli aspetti legali, che favorisca il raggiungimento degli obiettivi di efficienza nel rispetto della legislazione vigente.

Privacy e sicurezza

- Cosa si rischia se non implemento la sicurezza nella mia azienda? La risk analysis deve comprendere anche la risk analysis legale, troppo spesso dimenticata...!
- Implementazione della sicurezza...anche STRUMENTALE al raggiungimento della conformità alla legislazione!
- Sicurezza dei dati e dei sistemi:
 - Sicurezza fisica: protezione delle aree e dei locali; protezione della rete!
 - Sicurezza logica: protezione della rete!
 - Sicurezza organizzativa: istruzioni, procedure di sicurezza!

Il D. Lgs. 196/2003

- Fino al 31 dicembre 2003:
 - L. 31 dicembre 1996 n. 675 (e successive modificazioni e integrazioni, in particolare introdotte dal D. Lgs. 467/2001)
 - D.P.R. 28 luglio 1999 n. 318
- Dal 1° gennaio 2004:
 - “Codice in materia di protezione dei dati personali”, contenuto nel D. Lgs. 30 giugno 2003 n. 196 che unisce in un unico corpo normativo tutte le disposizioni in materia di *privacy*.

La struttura del codice

- Il nuovo Codice in materia di protezione dei dati personali è suddiviso in tre parti + allegati:
 1. Disposizioni generali (settore pubblico e privato)
 2. Disposizioni relative a specifici settori (ambito giudiziario, forze di polizia, difesa e sicurezza dello Stato, ambito pubblico, settore sanitario, scopi storici e statistici, lavoro, sistema bancario finanziario e assicurativo, comunicazioni elettroniche, libere professioni, giornalismo, marketing)
 3. Tutela dell'interessato e sanzioni
 - [Allegati (A: Codici di condotta, B: Misure minime di sicurezza, C: trattamenti non occasionali in ambito giudiziario o per fini di polizia)]
- **Il Codice si applica a chiunque è stabilito nel territorio dello Stato, anche se i dati sono detenuti all'estero.**

Alcune definizioni

- **TRATTAMENTO:** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- **DATO PERSONALE:** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- **DATI IDENTIFICATIVI:** i dati personali che permettono l'identificazione diretta dell'interessato;
- **DATI SENSIBILI:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Altre definizioni: i soggetti

- **INTERESSATO:** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- **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;
- **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;
- **INCARICATO:** la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

Il principio di necessità – art. 3

- Chiunque ha diritto alla protezione dei dati personali che lo riguardano: SONO TUTELATE SIA LE PERSONE FISICHE CHE GIURIDICHE!
- PRINCIPIO DI NECESSITA': i sistemi e i programmi informatici dovranno essere configurati in modo da **ridurre al minimo l'utilizzazione dei dati personali e identificativi**. Sarà necessario escluderne l'uso se sussiste la possibilità di **1) rendere anonimo il dato; 2) identificare l'interessato solo in caso di necessità**. In concreto, ciò significa che il titolare del trattamento dovrà preventivamente adottare tutte le misure organizzative/informatiche necessarie per permettere l'accesso ai soli dati indispensabili all'attività lavorativa, addirittura anonimizzando i dati se possibile.

Il principio di necessità permea il Codice in ogni sua parte e il titolare del trattamento deve tenerlo in considerazione ogniqualvolta si trovi di fronte ad una scelta, sia essa di carattere organizzativo oppure tecnologico.

Alcune regole generali

- Diritto di accesso ai dati (art. 7 e ss.): agevolare l'accesso ai dati personali da parte dell'interessato, semplificare le modalità e ridurre i tempi per il riscontro.
- Regole per il trattamento dei dati (art. 11) liceità, correttezza, pertinenza agli scopi, esattezza, conservazione limitata nel tempo secondo le finalità dichiarate.
- Informativa (art. 13):
 - Finalità/modalità trattamento dati
 - Natura obbligatoria/facoltativa conferimento dati
 - Conseguenze eventuale rifiuto di rispondere
 - Coloro (siano anche responsabili o incaricati) ai quali i dati personali possono essere comunicati e ambito di diffusione dei dati
 - Diritti di cui all'art. 7 (accesso)
 - Estremi del titolare/rappresentante territorio dello Stato/responsabile
- Consenso (artt. 23): libero, specifico, informato, documentato per iscritto. Se il trattamento riguarda dati sensibili, il consenso deve essere manifestato in forma scritta.
- Casi di esclusione dal consenso: art. 24 (dati personali) e art. 26 (i dati sensibili).
- **N.B.: NON ESISTONO CASI DI ESCLUSIONE DALL'INFORMATIVA!!!**

La notificazione (art. 37 – 38)

- La notificazione deve essere presentata prima dell'inizio del trattamento, una sola volta e SOLO SE SI RICADE IN UNA DELLE FATTISPECIE PREVISTE DALL'ART. 37.
- Deve necessariamente essere trasmessa in via telematica sul modello predisposto dal Garante.
- Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o se mutano talune delle condizioni da indicare nella notificazione medesima.
- Termine per la ri-notificazione: 30 aprile 2004
- REGISTRO DELLE NOTIFICAZIONI: consultabile online sul sito www.garanteprivacy.it.

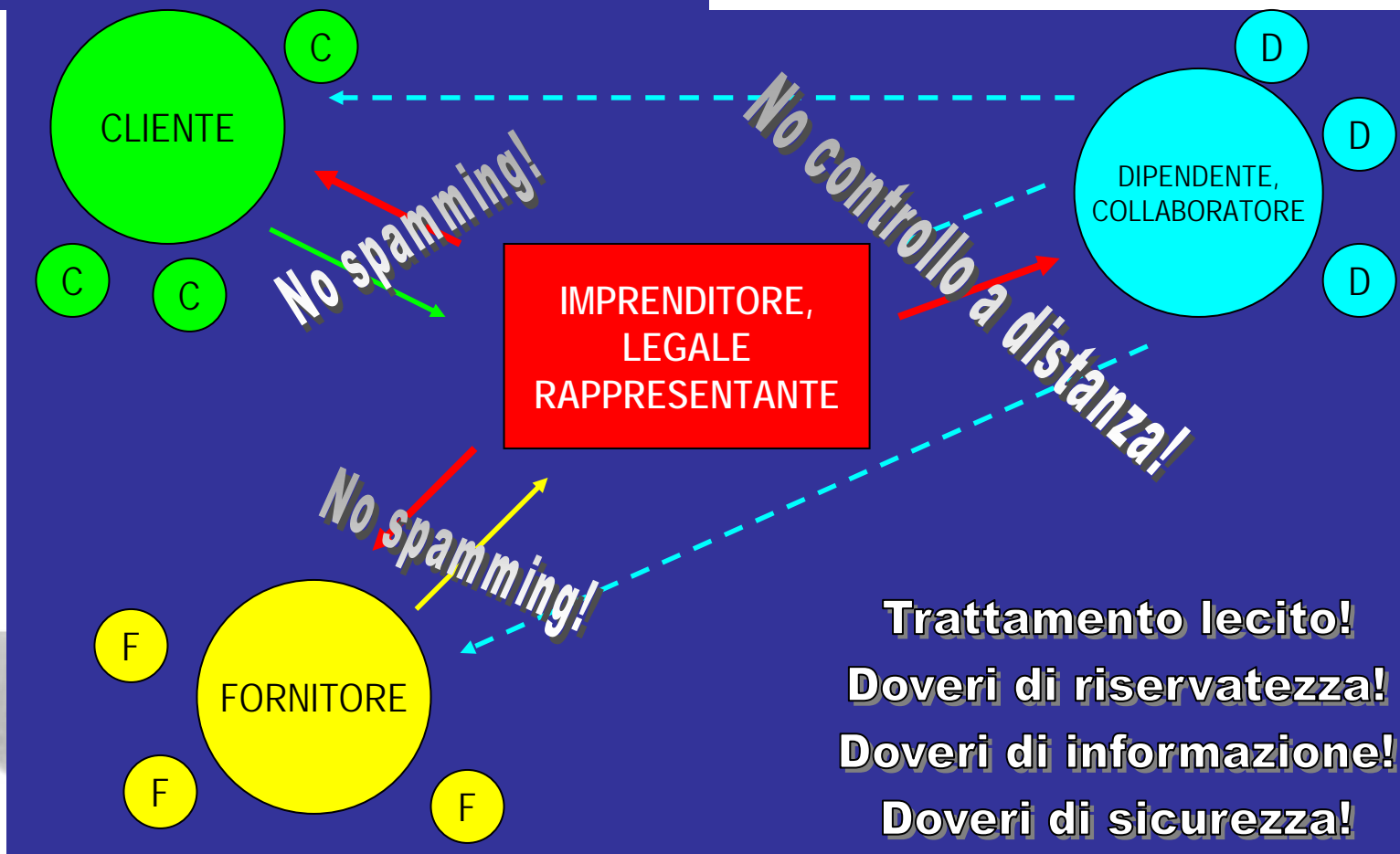
Chi deve notificare (art. 37)

- Scompare l'obbligo generale di notificazione: i casi di notificazione sono indicati chiaramente dal Garante:
 - Dati genetici, biometrici o dati che indichino la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
 - Dati idonei a rivelare lo stato di salute, a fini di procreazione assistita,...
 - Dati idonei a rivelare la vita sessuale o la sfera psichica,...
 - Dati trattati con strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
 - dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi; dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
 - dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Il trasferimento dei dati all'estero (artt. 42-45)

- All'interno dell'Unione Europea i dati personali possono circolare liberamente nel rispetto della legislazione in materia.
- Il trasferimento di dati verso un Paese terzo è consentito solo in determinati casi. Tra gli altri, se c'è il consenso espresso dell'interessato (in forma scritta se i dati sono sensibili), se è necessario per la salvaguardia della vita o dell'incolumità di un soggetto, se è autorizzato dal Garante in base a determinate garanzie per i diritti dell'interessato.
- Al di fuori di questi casi, il trasferimento è sempre vietato se il Paese di destinazione o di transito dei dati non assicura un adeguato livello di tutela.

Diritti e doveri di privacy



Divieto di controllo a distanza (art. 114)

- Resta fermo quanto previsto dall'art. 4 della L. 20 maggio 1970 n. 300.
 - È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.
 - Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.
 - Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

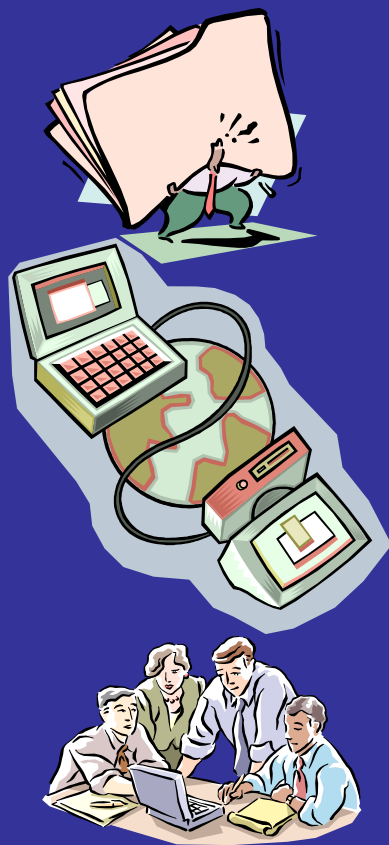
Comunicazioni indesiderate (spamming) – art. 130

- L'uso di sistemi automatizzati di chiamata per invio di materiale pubblicitario o commerciale è consentito solo con il consenso dell'interessato.
- È consentito l'invio di e-mail, telefax, mms, sms commerciali e pubblicitari solo agli utenti che abbiano espressamente dato il proprio consenso.
- Ulteriori comunicazioni con mezzi diversi ma stessi fini: consentite ai sensi degli artt. 23 e 24.
- Se il titolare del trattamento utilizza, a fini di vendita di prodotti/servizi, l'indirizzo di posta elettronica fornito dall'interessato nel contesto della vendita di un prodotto/servizio, può non richiedere il consenso, se si tratta di servizi analoghi a quelli oggetto della vendita e l'interessato, informato, non rifiuti tale uso, inizialmente o in seguito. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata, deve essere informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente. Tali operazioni non possono avvenire tramite l'uso di sistemi automatizzati di chiamata.
- E' vietato l'invio di comunicazioni per finalità commerciali o comunque promozionali, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di accesso.
- In caso di reiterata violazione di questi obblighi, il Garante può obbligare i fornitori di servizi di comunicazione elettronica ad adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

La sicurezza dei dati e dei sistemi (artt. 31-36)

- MISURE IDONEE E MISURE MINIME DI SICUREZZA:
 - I dati personali devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
 - Il livello minimo di sicurezza è garantito mediante l'applicazione delle misure minime elencate negli artt. 34 e 35 ed esplicitate nel disciplinare tecnico del Codice (Allegato B).

Misure idonee e misure minime



MISURE MINIME DI SICUREZZA

*Sanzioni amministrative!
Sanzioni penali!*



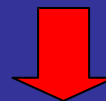
IDONEE E PREVENTIVE MISURE DI SICUREZZA

Responsabilità civile



Le misure idonee (art. 31)

- Non esistono parametri minimi di valutazione dell'idoneità, se non il “progresso tecnico” e *l'importanza* dei dati trattati...(art. 31)
- Chiunque cagiona ad altri danno per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c. (esercizio di attività pericolose), “se non prova di aver adottate tutte le misure idonee ad evitare il danno” (art. 15).



- **INVERSIONE DELL'ONERE DELLA PROVA!**

Le misure minime (artt. 33-35)

ART. 34: mezzi elettronici

- autenticazione informatica;
- procedure di gestione delle credenziali di autenticazione;
- sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
- protezione dei documenti elettronici e dei dati;
- procedure di backup;
- Piano Nazionale Programmatico sulla Sicurezza Informatica;
- l'uso di cifratura o codici identificativi per trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

ART. 35: sicurezza mezzi elettronici

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
- procedure per idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Livello minimo di protezione dei dati

Il dettaglio...nell'Allegato B

TRATTAMENTO

CON L'AUSILIO DI MEZZI ELETTRONICI

- Sistema di autenticazione informatica
- Sistema di autorizzazione
- Altre misure di sicurezza
- Documento Programmatico sulla Sicurezza
- Ulteriori misure per dati sensibili o giudiziari
- Misure di tutela e garanzia

SENZA L'AUSILIO DI MEZZI ELETTRONICI

- Istruzioni scritte agli incaricati per vigilanza (controllo e custodia), per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e documenti contenenti dati personali.
- Particolare attenzione per documenti e atti contenenti dati sensibili e giudiziari consegnati all'incaricato: controllo e custodia affinché non vi accedano persone prive di autorizzazione, restituzione al termine delle operazioni affidate.
- L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato. Dopo l'orario di chiusura, le persone ammesse devono essere identificate e registrate. Se gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati alla vigilanza, le persone che vi accedono devono essere preventivamente registrate.

Sistema di autenticazione informatica (punti 1-11)

- **CREDENZIALI DI AUTENTICAZIONE + PROCEDURA DI AUTENTICAZIONE:**
 - Codice identificativo + parola chiave riservata oppure
 - Dispositivo di autenticazione in possesso ed uso esclusivo dell'incaricato, eventualmente associato ad un codice identificativo/parola chiave oppure
 - Caratteristica biometrica dell'incaricato eventualmente associata ad un codice identificativo/parola chiave
- Ad ogni incaricato possono essere associate una o più credenziali
- Le credenziali non utilizzate per almeno sei mesi (se non sono preventivamente autorizzate per scopi di gestione tecnica) o in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali devono essere disattivate.
- **LA PAROLA CHIAVE:**
 - È composta da almeno 8 caratteri oppure da un numero di caratteri pari al massimo consentito se il sistema non lo consente.
 - Non deve contenere riferimenti agevolmente riconducibili all'incaricato.
 - Deve essere modificata dall'incaricato al primo utilizzo e successivamente, almeno ogni sei mesi (tre mesi se il trattamento riguarda dati sensibili o giudiziari).
- **IL CODICE PER L'IDENTIFICAZIONE:**
 - Non può essere assegnato ad altri incaricati neppure in tempi diversi.

Sistema di autenticazione informatica (punti 1-11)

- **OBBLIGHI PER L'INCARICATO**

- La componente riservata della credenziale deve essere mantenuta segreta
- I dispositivi in possesso devono essere diligentemente custoditi
- Lo strumento elettronico, durante una sessione di trattamento, non deve essere lasciato incustodito e accessibile.

QUESTE ISTRUZIONI DEVONO ESSERE IMPARTITE PER ISCRITTO A CURA DEL TITOLARE O DEL RESPONSABILE!

- Altresì devono essere impartite idonee e preventive disposizioni scritte volte ad individuare le modalità con le quali i dati e gli strumenti elettronici possono essere resi disponibili in caso di prolungata assenza o impedimento dell'incaricato che renda **INDISPENSABILE E INDIFFERIBILE** intervenire per **ESCLUSIVE NECESSITÀ DI OPERATIVITÀ E DI SICUREZZA DEL SISTEMA**.
- La custodia delle credenziali deve essere organizzata garantendone la segretezza e individuando per iscritto i soggetti incaricati della custodia delle chiavi, che devono informare tempestivamente l'incaricato in caso di intervento effettuato.

Sistema di autorizzazione (punti 12-14)

- I profili di autorizzazione devono essere individuati e configurati
 - Per ciascun incaricato o classi omogenee di incaricati
 - Anteriormente all'inizio del trattamento
 - Limitando l'accesso ai soli dati necessari per effettuare le operazioni di trattamento
- Periodicamente e comunque almeno una volta all'anno deve essere verificata la sussistenza delle condizioni per la conservazione dei profili di autenticazione.
- In questo ambito, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e relativi profili di autorizzazione.

Altre misure di sicurezza

- E' necessario attivare idonei strumenti elettronici da aggiornare con cadenza almeno semestrale per proteggere i dati personali da rischi di intrusione e azione di programmi di cui all'art. 615-quinquies c.p..
 - Virus, worms,...
- Aggiornamenti periodici dei programmi di protezione per prevenire vulnerabilità e correggere difetti: almeno annualmente. Se il trattamento riguarda dati sensibili: almeno semestralmente.
- Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
- Se le misure minime di sicurezza sono adottate tramite soggetti esterni, l'installatore deve consegnare una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni dell'Allegato B.

Il Documento Programmatico sulla Sicurezza (punto 19)

- Solo i titolari di trattamenti di dati sensibili o giudiziari devono predisporre il D.P.S e non esiste più la distinzione tra reti accessibili e non accessibili al pubblico.
- Il D.P.S. deve essere redatto la prima volta entro il 30 giugno 2004 e poi aggiornato entro il 31 marzo di ogni anno.
- Il titolare del trattamento riferisce, nella relazione accompagnatoria al bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del D.P.S. (punto 26 dell'allegato B).
- Il D.P.S. deve essere disponibile in azienda per un eventuale controllo da parte dell'Autorità. Non deve essere inviato al Garante.

Documento Programmatico sulla Sicurezza

- Nel D.P.S. devono essere indicati:
 - L'elenco dei trattamenti effettuati
 - La distribuzione dei compiti e delle responsabilità
 - L'analisi dei rischi
 - Le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali
 - La descrizione dei criteri e delle modalità di ripristino della disponibilità dei dati in caso di distruzione o danneggiamento
 - Il piano di formazione degli incaricati
 - La descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti effettuati all'esterno della struttura del titolare.
 - I criteri da adottare per la cifratura/separazione dei dati sensibili dagli altri dati personali dell'interessato (organismi sanitari)

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari (punti 20-24)

- I dati sensibili e giudiziari devono essere protetti contro gli accessi abusivi (art. 615 ter) con idonei strumenti informatici.
- Devono essere impartite istruzioni adeguate organizzative e tecniche per la custodia e l'uso dei supporti rimovibili dove risiedono i dati per evitare accessi non autorizzati e trattamenti non consentiti
- I supporti rimovibili contenenti i dati non utilizzati devono essere distrutti o resi inutilizzabili. Possono essere riutilizzati da chi non è autorizzato al trattamento solo se le informazioni contenute non sono intelligibili e tecnicamente ricostruibili
- Ripristino dell'accesso dei dati in caso di danneggiamento degli stessi/degli strumenti elettronici: entro tempi certi compatibili con i diritti dell'interessato e comunque entro 7 giorni
- Per organismi/esercenti sanitari: trattamento disgiunto di dati sensibili/dati identificativi dell'interessato. Dati genetici: locali protetti e accesso a incaricati specificamente autorizzati; trasporto dati all'esterno: contenitori muniti di serratura o dispositivi equipollenti; trasferimento dati in formato elettronico: cifrato.

Tutela amministrativa e giurisdizionale (artt. 141-152)

- Amministrativa: davanti al Garante
 - Reclami
 - Segnalazioni
 - Ricorsi
- Giurisdizionale: davanti all'Autorità giudiziaria competente
 - Ricorso presentato alla cancelleria del Tribunale competente (quello dove risiede il titolare del trattamento)
 - Il Tribunale decide sempre in composizione monocratica

Le sanzioni (artt.161-172)

...AMMINISTRATIVE

VIOLAZIONE	RIFERIMENTI	SANZIONE
Omessa o inidonea informativa all'interessato (art. 161)	Artt. 13, 17, 26, 27	Da 3.000 a 18.000 Euro se dati personali. Da 5.000 a 30.000 Euro se dati sensibili. Aumento fino al triplo se inefficacia in ragione delle condizioni economiche dell'interessato. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Cessione di dati (art. 162 comma 1)	Art. 16	Da 5.000 a 30.000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Comunicazione dei dati all'interessato da parte di altri rispetto al medico designato dal titolare o dall'interessato (art. 162 comma 2)	Art. 84	Da 500 a 3000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Omessa o incompleta notificazione (art. 163)	Artt. 37, 38	Da 10.000 a 60.000 Euro e pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.
Omessa informazione o esibizione al Garante (art. 164)	Artt. 150, 157	Da 4.000 a 24.000 Euro. Possibile pubblicazione dell'ordinanza-ingiunzione su uno o più giornali indicati nel provvedimento stesso.

Le sanzioni (artt.161-172)

...PENALI

VIOLAZIONE	RIFERIMENTI	SANZIONE
Trattamento illecito di dati (art. 167 comma 1) (tra gli altri, trattamento senza il consenso dell'interessato)	Artt. 18, 19, 23, 123, 126, 129, 130	Reclusione da 6 a 18 mesi. Se si tratta di comunicazione o diffusione di dati, da 6 a 24 mesi. Pubblicazione della sentenza.
Trattamento illecito di dati (art. 167 comma 2) (tra gli altri, violazione delle norme sui dati sensibili)	Artt. 17, 20, 21, 22, 25, 26, 27, 45	Reclusione da 1 a 3 anni. Pubblicazione della sentenza.
Falsità nelle dichiarazioni e notificazioni al Garante (art. 168)	Art. 37	Reclusione da 6 mesi a 3 anni. Pubblicazione della sentenza.
Misure minime di sicurezza (art. 169)	Art. 33	Arresto fino a 2 anni o ammenda da 10.000 a 50.000 Euro. Prescrizione Garante: termine per la regolarizzare (max 6 mesi). Se risulta adempimento: l'autore del reato è ammesso a pagare un quarto del massimo dell'ammenda stabilita. L'adempimento e il pagamento estinguono il reato.
Inosservanza di provvedimenti del Garante (art. 170)	Artt. 26, 90, 143, 150	Reclusione da 3 mesi a 2 anni. Pubblicazione della sentenza.
Violazione del divieto di indagine sulle opinioni dei lavoratori e del controllo a distanza (art. 171)	Art. 113, 114	Arresto da 15 giorni a 1 anno o ammenda da 51 a 516 Euro. casi più gravi: arresto e ammenda applicati congiuntamente e sentenza pubblicata. Facoltà di aumentarla fino al quintuplo per condizioni economiche del reo.

Scadenziere

31 marzo 2004 <u>SOLO PER IL 2004 LA SCADENZA E' AL 30 GIUGNO!</u>	Documento Programmatico sulla Sicurezza	Allegato b) punto 19
30 aprile 2004	Notificazioni	Art. 181 c. 1 lett. c)
30 giugno 2004	Nuove misure di sicurezza	Art. 180 c.1
30 giugno 2004	Documento avente data certa per proroga applicazione misure minime di sicurezza	Art. 180 c. 2
31 dicembre 2004	Adeguamento in caso di proroga ex. art. 180 c.2	Art. 180 c.3

GRAZIE PER L'ATTENZIONE!

STUDIO GENGHINI & ASSOCIATI

Via S. Pietro all'Orto, 17

20121 Milano

tel +39 02 7630301

fax +39 02 76303029

e.security@sng.it

www.genghinieassociati.it

