genesys
software srl

SISTEMI INFORMATIVI
Via Rodolfo Redi, 3 - 70124 BARI
Tel. 080/561.90.01 Fax 080/561.43.91
E-mail: genesys@genesysnet.it

Privacy

Argomenti della presentazione

PRIVACY

IL CODICE SULLA PRIVACY

INTRODUZIONE

Il decreto legislativo n. 196/2003, che il 22 Dicembre 2005, è stato ribattezzato "Decreto Milleproroghe", afferma il principio per cui chiunque ha diritto alla tutela dei dati personali che lo riguardano. Esso ha introdotto importanti novità in molti campi professionali e aziendali e ha stabilito che i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di dati personali e identificativi.

Il codice sulla privacy garantisce:

- **Diritti e libertà**
- **La dignità dell'interessato**
- **La presentazione dei dati personali**

CHI DEVE ADEMPIERE AI NUOVI OBBLIGHI?

Chiunque tratta dati personali, cioè:

- Aziende
- Professionisti e Ordini professionali
- Cooperative e Associazioni
- Pubblica Amministrazione, Enti Pubblici, Comuni
- Scuole
- Ospedali

DEFINIZIONI IMPORTANTI

Dati personali: trattasi di informazioni relative a persona fisica, persona giuridica, ente, associazione, identificate o identificabili.

Dati identificativi: permettono l'identificazione diretta dell'interessato.

Dati giudiziari: informazioni che rivelano la qualità di imputato o di indagato del soggetto e indicazioni contenute nel casellario giudiziale

Dati sensibili: rivelano l'origine razziale ed etnica, le convinzioni religiose, politiche, filosofiche, l'adesione a partiti o ad associazioni e sindacati, nonché quelli idonei a rivelare lo stato di salute e la vita sessuale.

Titolare: è la persona fisica, la persona giuridica, la pubblica amministrazione, qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile: è il soggetto preposto dal titolare al trattamento dei dati personali. Il responsabile, deve procedere al trattamento dei dati attenendosi alle istruzioni impartite per iscritto dal titolare.

Trattamento: Qualunque operazione, o complesso di operazioni, effettuata anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, la modifica, l'elaborazione, la cancellazione la diffusione, il raffronto, l'utilizzo, il blocco e la distruzione dei dati, anche se non registrati in una banca dati.

IMPORTANZA DEL CODICE:

Migliorare l'organizzazione ed i processi aziendali

Ottimizzare la gestione ed il controllo sulla sicurezza delle informazioni

Con la nuova normativa diventa sempre più necessario assolvere non solo ad oneri burocratici, ma soprattutto creare una nuova cultura della Privacy, attraverso strumenti più complessi delle semplici informative e richieste di consenso.

Questo, pertanto, è il momento giusto per le aziende di fare un salto qualitativo e trasformare l'incombenza in un valore aggiunto. Per esempio, delineare una trasformazione tecnologica integrata con i processi e con l'organizzazione; disegnare un modello architetturale in base alle singole esigenze, tenendo sempre presente, ovviamente, i costi operativi; e, infine, sviluppare un documento tecnico e organizzativo che consente di adeguarsi alle richieste del Nuovo Codice.

È' necessario, dunque, creare le condizioni ottimali in azienda affinché si possano minimizzare i costi derivati da una gestione non razionale e non corretta dei dati e della loro trasmissione, proteggere e valorizzare i dati personali in proprio possesso, cioè il patrimonio aziendale, trasmettere a terzi un immagine di correttezza, trasparenza e particolare attenzione ai propri interlocutori interni ed esterni, operare con maggiore efficienza e funzionalità .

E' evidente che questa normativa lega in modo indissolubile problematiche di tecnologia e di natura legale, amministrativa, organizzativa, per porre poi nuove basi di business aziendale.

SANZIONI

Nel Testo Unico vige il principio della responsabilità per il trattamento dei dati personali. In base a questo principio chi cagiona un danno ad altri per il trattamento dei dati personali è tenuto al risarcimento se non prova di aver adottato tutte le misure tecniche ed organizzative idonee ad evitare il danno:

Sanzioni amministrative:

Da 3.000 a 18.000 euro (ovvero da 5.000 a 30.000 euro nei casi di dati sensibili o giudiziari o che presentano rischi specifici), aumentabile sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

Da 10.000 a 60.000 euro, oltre alla sanzione accessoria della pubblicazione dell'ordinanza/ingiunzione su uno o più giornali (**Notificazione omessa o incompleta)**.

Da 4.000 a 24.000 euro per omessa informazione o esibizione al Garante.

Sanzioni penali:

per trattamento illecito di dati: reclusione da sei mesi a 3 anni;

per false dichiarazione o comunicazione al Garante: reclusione da sei mesi a 3 anni;

per omessa adozione delle misure minime di sicurezza: arresto fino a 2 anni o sanzione amministrativa (pagamento di una somma da 10.000 a 50.000 euro).

per inosservanza dei provvedimenti del Garante: reclusione da 3 mesi a 2 anni.

QUALI SONO GLI ADEMPIMENTI A CARICO DEL TITOLARE:

Organizzativi:

- Individuare i soggetti coinvolti nel processo di trattamento dei dati (titolare, responsabile, incaricato).
- Specificare per iscritto i compiti affidati al responsabile.
- Nominare per iscritto gli incaricati e sempre per iscritto individuare i compiti e l'ambito del trattamento consentito.
- Vigilare sull'osservanza delle disposizioni e istruzioni.

Nei confronti dell'interessato:

- Fornire all'interessato l'informativa
- Acquisire il consenso dell' interessato al trattamento dei propri dati personali

Nei confronti del Garante:

- Notificare all'Autorità Garante alcune tipologie di trattamenti di dati personali (art.37).

- Richiedere l'autorizzazione per il trattamento di alcune tipologie di dati (art.41).
- Comunicare particolari circostanze (art.39).

Relativi alle misure minime di sicurezza:

Adottare le misure di sicurezza minime con attenzione alla redazione del Documento Programmatico sulla Sicurezza (DPS).

LA NOTIFICAZIONE DEL TRATTAMENTO

La notificazione consiste in un modello, in cui vengono dichiarati i trattamenti effettuati, le modalità e le finalità del trattamento, le misure di sicurezza adottate, da inviare in via telematica al Garante prima dell' inizio del trattamento, ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento.

Contrariamente a quanto avveniva in passato, il titolare deve ora procedere ad inviare la notificazione solo nei casi previsti dalla norma (art. 37), vale a dire quando il trattamento riguarda principalmente dati relativi alla salute, alla sfera sessuale o psichica, dati volti a definire il profilo o la personalità, dati ai fini della selezione del personale, dati relativi a sondaggi di opinione e ricerche di mercato, dati relativi alla solvibilità economica o alla situazione patrimoniale degli interessati.

ADEMPIMENTI RELATIVI ALLE MISURE MINIME DI SICUREZZA

Quali sono le misure minime di sicurezza?

I. Autenticazione Informatica:

Autenticazione Informatica

È il procedimento con il quale un utente viene riconosciuto come tale. In un sistema informatico ci sono varie forme di autenticazione e il disciplinare tecnico (allegato b) chiarisce la necessità che ogni incaricato debba essere munito di una o più credenziali di autenticazione (cioè, i dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per autenticazione informatica).

Ogni volta che un incaricato effettua un trattamento dati deve essere dotato di credenziali di autenticazione per effettuare una procedura di autenticazione.

Le credenziali di autenticazione consistono in:

a) un codice di identificazione (user-id o login) dell' incaricato, associato a una parola chiave (password) riservata, conosciuta solamente dal medesimo;

b) un dispositivo di autenticazione in possesso ad uso esclusivo dell'incaricato;

c) in una caratteristica biometria dell'incaricato (per esempio l'impronta digitale, l'iride, la retina).

Le credenziali di autenticazione debbono essere composte:

a) Di almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Non deve contenere riferimenti agevolmente riconducibili all'incaricato.

b) Devono essere modificate dall'incaricato al primo utilizzo e, successivamente, ogni sei mesi. In caso di trattamento di dati sensibili e giudiziari la parola chiave va modificata ogni tre mesi.

c) Devono essere assegnate individualmente.

d) La componente riservata (password) non può essere comunicata a terzi.

Le credenziali di autenticazione devono essere disattivate:

a) quando non vengono utilizzate da almeno sei mesi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. In questo caso ci riferiamo ad interventi tecnici che avvengono con periodicità molto lunga, tipo quelli di manutenzione hardware o software.

b) In caso di perdita della qualità delle credenziali.

Adozione di procedure di gestione delle credenziali di autenticazione:

Il titolare deve prescrivere agli incaricati istruzioni puntuali per assicurare la segretezza della componente riservata della credenziale di autenticazione e per non lasciare incustodito e accessibile il terminale (PC, server, o altro strumento elettronico).

Il titolare deve fornire agli incaricati istruzioni per la procedura da eseguire nel caso in cui l'incaricato sia irreperibile e per l'organizzazione e gestione delle credenziali di autenticazione.

II) Sistema di Autorizzazione:

E' l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Utilizzazione di un profilo di autorizzazione:

Un sistema informatico dopo aver autenticato una persona, cerca il suo profilo di autorizzazione:

I profili di autorizzazione:

Possono essere definiti per ciascun incaricato o per classi omogenee di incaricati.

Devono essere individuati e configurati prima dell'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento

Periodicamente deve essere verificata la validità e sussistenza delle condizioni per la conservazione dei profili di autorizzazione. Questa procedura deve essere effettuata almeno annualmente.

E' sempre necessario ricorrere ad un sistema di autorizzazione?

Il disciplinare tecnico (Allegato B) al riguardo chiarisce che:

- nel caso siano individuabili ambiti diversi di trattamento in modo da limitare l'accesso dell'incaricato ai soli dati necessari per effettuare le operazioni di trattamento;
- non si deve utilizzare un sistema di autenticazione quando trattiamo dati destinati alla diffusione.

III) Manutenzione e Aggiornamento

Il disciplinare tecnico definisce una serie di regole per un coretto mantenimento del sistema poiché la sicurezza deve essere un processo che ha bisogno di una corretta manutenzione e un continuo aggiornamento.

In questa categoria rientrano due misure minime di sicurezza previste dal codice:

a) Aggiornamento periodico dell'individuazione nell' ambito del trattamento consentito ai singoli incaricati e addetti alla gestione e alla manutenzione degli strumenti elettronici.

All'intero sistema deve essere effettuato un aggiornamento periodico (almeno annualmente) e, se necessario, riorganizzare gli ambiti e la relativa lista degli incaricati (gestione delle scadenze).

b) Adozione di procedure per la custodia di copie di sicurezza, ripristino della disponibilità dei dati e dei sistemi. Munirsi, pertanto, di procedure e sistemi che annullino la possibilità di perdere dei dati.

L'organizzazione deve munirsi di procedure per il salvataggio dei dati per produrre copie di sicurezza. E' indispensabile che le imprese pensino seriamente alle conseguenze che alcuni eventi possono determinare nella vita dell'azienda per poter prendere le precauzioni necessarie.

I rischi possono essere sia esterni che interni. I punti su cui concentrare l'attenzione quando si deve redigere un piano di analisi dei rischi e i **disaster recovery** sono vari:

- integrità fisica dei sistemi informatici (che possono essere calamità naturali (alluvioni, terremoti) cause accidentali (incendi, allagamenti) o cause esterne (furto devastazione)
- Integrità delle infrastrutture necessarie al funzionamento dei sistemi (elettricità, connettività di rete)
- Integrità dei dati (azioni di cracking, errori umani, virus, guasti hardware).

Importante precauzione per evitare i danni della perdita dei dati è il **backup** dei dati.

All'interno dell'azienda dovrà essere nominato un responsabile per il backup che dovrà provvedere al salvataggio periodico (almeno settimanale) dei dati aziendali.

Deve essere consentito di eseguire la copia su qualsiasi supporto (es.: cd o DVD) in maniera completamente automatica, inserendosi come procedura automatica all'interno dello scadenzario, gestito dal sistema operativo. Il responsabile delle copie deve poi custodire il supporto in un luogo sicuro.
Deve essere previsto un ripristino in tempi brevissimi di una copia effettuata.

I dati devono essere protetti da password e criptati in maniera che nessuno, venendone in possesso, può utilizzarli per scopi non leciti.

IV) Altre Misure Di Sicurezza

a) **Protezione degli strumenti elettronici e dei dati** rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici (Soluzione di protezione Hardware e Software)

b) **Gli aggiornamenti periodici dei programmi** per elaboratori volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne i difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è semestrale.

c) **Aggiornare il software è un obbligo di legge**, ed è quindi necessario che vengano istallate le pacht e i service pack rilasciati. Quindi, se nel vostro intervento adeguate i sistemi informatici, dovrete periodicamente prevedere il download e l'istallazione delle pacht.

d) **E' evidente che l'obbligo di aggiornamento dei sistemi informatici** rende obsoleti alcuni dei più comuni sistemi Windows, come Windows95, WIN98, WINNT4, WIN ME.

e) Un altro importante strumento obbligatorio per legge è **l'antivirus**. L'antivirus è obbligatorio indipendentemente dal fatto che il computer sia collegato a internet.

f) E' obbligatorio anche il **firewall**, un sistema di protezione da intrusioni nella rete.

V) Ulteriori misure in caso di dati sensibili o giudiziari

Il codice stabilisce che :

- **I dati sensibili, o giudiziari, devono essere protetti contro l'accesso abusivo, mediante strumenti elettronici.**
- **inoltre dispone una serie di obblighi, quali:**
  - ✓ **Impartire istruzioni organizzative e tecniche** per la custodia e l'uso dei supporti rimovibili (cd,dvd, in cui sono memorizzati i dati) al fine di evitare accessi non autorizzati e trattamenti illeciti.
  - ✓ **I supporti rimovibili contenenti dati sensibili o giudiziari**, se non utilizzati, sono distrutti o resi inutilizzabili
  - ✓ **Garantire la disponibilità dei dati nei tempi compatibili con gli interessati**, per cui, in caso di danneggiamento dei dati, bisogna provvedere a procedure e processi che ripristino i dati nei tempi stabiliti.

MISURE DI TUTELA E GARANZIA

Il titolare che si avvale di soggetti terzi, quali società o professionisti del settore, per rendere conforme la sua organizzazione al testo unico della privacy, deve provvedere a farsi rilasciare una descrizione scritta di quali sono stati gli interventi che ne attestino la conformità con la normativa, nel caso particolare, con l'Allegato B.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

REQUISITI

Questo adempimento è previsto esclusivamente per i soggetti che trattano dati sensibili o giudiziari in forma elettronica. Con l' ultima proroga avranno tempo fino al 31 marzo 2006 per adottare le nuove "misure minime "di sicurezza a salvaguardia dei dati personali" contenuti negli archivi e per redigere il documento programmatico in materia di sicurezza.

Il D.P.S è un manuale per la pianificazione della sicurezza dei dati in azienda: descrive come si tutelano i dati personali dei dipendenti, collaboratori, clienti, utenti, fornitori, ecc.

Lo scopo del D.P.S è proprio quello di descrivere la situazione attuale con riferimento ai punti stabiliti dal Garante. I punti contenuti in esso rappresentano una "foto" istantanea dell'azienda, e, quindi,di un dato momento storico. Ognuna delle misure e delle attribuzioni delle responsabilità può essere oggetto di modifiche e integrazioni nel corso del tempo, considerando soprattutto l'obsolescenza degli strumenti informatici.
Il documento può essere redatto dal Titolare, anche attraverso il responsabile del trattamento (se designato) e deve contenere le seguenti informazioni (Allegato B):

1) **Elenco dei trattamenti di dati personali**
   Individuare 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.

2) **Distribuzione dei compiti e delle responsabilità**
   Descrizione sintetica dell' 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

3) **Analisi dei rischi che incombono sui dati**
   Descrivere in questa sezione i principali eventi potenzialmente dannosi per la sicurezza dei dati, e valutarne le possibili conseguenze e la gravita in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

4) Misure in essere da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

Riportare , 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. Per esempio occorrerà che il responsabile del trattamento verifichi che gli incaricati provvedano a cambiare la propria password nei tempi e termini stabiliti.

Le misure di sicurezza generalmente adottate sono:

- installazione di antivirus;
- installazione del firewall ;
- password di autenticazione;
- chiusura a chiave dei schedari;
- custodia in luogo sicuro di supporti rimovibili (floppy disk,CD, DVD) su cui erano memorizzati dati non utilizzati.

5) Criteri e modalità di ripristino della disponibilità dei dati

Prevede la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento. Al fine di limitare i danni , occorre predisporre delle procedure che garantiscono il ripristino dei dati distrutti o danneggiati. Si tratta di indicare all' interno del documento le procedure che in genere comunque previste al fine di evitare che il lavoro compiuto venga perduto. Infine, occorre prevedere interventi periodici di manutenzione da parte di tecnici o altro personale professionalmente adeguato.

6) Pianificazione degli interventi formativi previsti

Indica la previsione di interventi formativi degli incaricati del trattamento , sia al momento dell' ingresso in servizio, sia in occasione di cambiamenti di mansioni , o di introduzione di nuovi significativi strumenti , rilevanti rispetto al trattamento dei dati personali.
Le persone a cui viene affidato il trattamento dei dati, oltre a dover essere affidabili , devono anche avere le necessarie capacità professionali. Per questo è indispensabile prevedere degli interventi formativi sia al momento del conferimento dell' incarico , sia ogni volta che si introducano novità negli strumenti utilizzati per il trattamento dei dati personali ,o nel tipo di trattamento.

Il criterio è mettere le persone incaricate del trattamento in grado di svolgere correttamente il compito che è stato loro attribuito. Nel caso in cui le conoscenze tecniche degli incaricati siano scarse ovvero le modalità del trattamento dei dati siano complesse, sarà necessario rivolgersi a professionisti esterni.

7) Trattamenti affidati all' esterno

Prevede la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati ,in conformità al codice, all' esterno della struttura del titolare. Affidare il trattamento dei dati a terzi all' organizzazione non esime il titolare e il responsabile del trattamento dall' accertarsi che il terzo incaricato adotti le misure minime di sicurezza.
Per questo,al momento della stipulazione del contratto, l' organizzazione provvederà a richiedere una dichiarazione contenente tutte le previsioni indicate dal Garante , in cui il soggetto esterno attesterà tra le altre cose di aver redatto il proprio D. P. S e aver adottato le altre misure minime previste dall' Allegato B del Codice.

8) **Cifratura dei dati o separazione dei dati identificativi**

Chiede l'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale degli altri dati personali dell' interessato.
Questo aspetto riguarda solo i soggetti che rivestano la qualifica di organismi sanitari e esercenti professioni sanitarie.

I tempi di stesura del D.P.S variano a seconda della dimensione dell' azienda e dalla mole dei dati da processare. Il Documento Programmatico richiede un'attenta valutazione della situazione aziendale e dei trattamenti effettuati. La Legge sulla Privacy stabilisce che il D.P.S debba essere rinnovato costantemente. La scadenza per l'aggiornamento da operare annualmente è il 31 Marzo.

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.

Come si compila:

Esiste un documento on line redatto dal Garante, oppure esistono sul mercato software che agevolano la compilazione del D.P.S.. In questo modo potrete assicurarvi una maggiore **correttezza, l'impossibilità di omettere dati obbligatori e una semplificazione del processo.**

TRATTAMENTO DEI DATI IN FORMA CARTACEA

Se il trattamento dei dati avviene in forma cartacea, il titolare dovrà:

- fornire l' informativa;
- ricevere il consenso;
- mettere in atto le misure di sicurezza contemplate nel codice (art. 35)