GP&A Srl
Via Seprio, 2
20149 Milano
Phone: 02/45.49.53.73
Fax: 02/45.49.53.74
Email: info@gpa.it

Consulenza sul Documento Programmatico sulla Sicurezza in ottemperanza al nuovo Testo Unico sulla Privacy

Gentile cliente,

Desideriamo informarla che lo scorso 1° Gennaio 2004, è entrato ufficialmente in vigore il Nuovo Codice "Protezione dei Dati Personali".

Tra gli argomenti principali viene trattato il problema dei requisiti che devono essere posseduti da un sistema informativo al fine di garantire la massima tutela dei dati personali trattati.

Il Garante, dopo aver considerato la complessità della nuova normativa ed i tempi molto stretti, che praticamente impedivano l'immediata applicazione delle norme, con successivi provvedimenti ha spostato al 30 giugno 2004 la data ultima entro la quale le aziende private avranno tempo per adottare le "misure minime" di sicurezza introdotte a salvaguardia dei dati personali contenuti nei propri archivi e per redigere il documento programmatico in materia di sicurezza.

GP&A intende proporre ai suoi clienti un servizio articolato che li aiuti ad orientarsi nello scenario normativo imposto dall'entrata in vigore della nuova Legge ed evitare di incorrere nelle sanzioni previste dal Codice.

Cosa è un “sistema informativo”?

Poiché nel nuovo codice viene trattato il tema “Sistemi Informativi” desideriamo immediatamente far presente che un “sistema informativo” non si identifica con un sistema informatico: un sistema informativo è l’insieme degli strumenti, delle risorse e delle procedure che consentono la gestione di ogni tipo di informazione all’interno dell’azienda:

- è essenziale per il funzionamento dell’azienda;
- è fortemente integrato con il sistema organizzativo;
- comprende risorse umane, generalmente ogni azienda ha un Sistema Informativo, anche se non viene definito in maniera esplicita;

Un sistema informatico è invece solamente l’insieme delle apparecchiature hardware e dei pacchetti software presenti in una azienda, che vengono utilizzati per la generazione, la raccolta, l’elaborazione, la memorizzazione di dati su supporti magnetici.

Ogni azienda, svolgendo quotidianamente la propria attività acquisisce una mole enorme e molto diversificata nei contenuti, di dati riguardanti tutte le persone fisiche o giuridiche con cui viene in contatto.

Il “dato”: è una unità elementare grezza che, elaborato da un sistema informatico secondo criteri ed esigenze specifiche diviene “informazione”, spesso molto sofisticata.

Con il trascorrere del tempo, la comunità ha avvertito con forza sempre maggiore l’esigenza di circoscrivere e limitare sempre più i campi e le modalità per l’utilizzo di questi dati da parte di coloro che ne venivano in possesso, al fine di garantire e tutelare la riservatezza e la privacy dei titolari dei diritti correlati a tali dati ed informazioni.

Proseguendo il suo cammino in questa direzione, il legislatore ha continuato ad intervenire con attenzione sempre maggiore mettendo a punto una serie di norme sempre più moderna, con leggi e provvedimenti tagliati sulle varie tipologie di informazioni e sulle modalità di utilizzo possibili ed ha ulteriormente rafforzato la tutela del diritto alla riservatezza ed alla “privacy” appartenenti a terze persone.

Il nuovo codice, entrato in vigore nel gennaio 2004 si pone la finalità di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dei titolari, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali.

GP&A Srl - Via Seprio, 2 - 20149 Milano - Tel: 02/45.49.53.73 Fax: 02/45.49.53.74 - Email: info@gpa.it

La procedura

La tipologia estremamente diversificata di soggetti sottoposti all'obbligo, in combinazione con una casistica di adempimenti decisamente articolata, in molti casi diversa da soggetto a soggetto, ci impone di strutturare il nostro intervento in tre diversi momenti:

- Una prima fase durante la quale il nostro personale specializzato durante una serie di visite presso il cliente, verificherà lo stato dell'arte, andrà ad identificare le attività previste dalla nuova normativa per l'adeguamento dell'attuale sistema informativo alla nuova normativa e predisporrà il report per responsabile delle operazioni della nostra società.
  I primi casi esaminati ci hanno permesso di effettuare una valutazione del costo di questa prima fase:

  - per "sistemi informativi di "bassa complessità", sono necessari ca. 3/4 giorni di intervento;

  - per "sistemi informativi di "media complessità" sono necessari ca. 6/8 giorni di intervento;

  - per "sistemi informativi di "elevata complessità" sono necessari almeno 10 giorni di intervento.

- Una seconda fase, che richiede mediamente 5 giorni lavorativi nella quale sarà studiato il tipo di intervento, eventuali apparecchiature hardware e pacchetti software necessari, saranno calcolate le ore lavoro necessarie al completamento ed al collaudo dell'intervento, le ore necessarie per lo studio delle procedure, per la produzione della documentazione richiesta, eventuali tempi di approvvigionamento e saranno approntati il calendario di intervento e la quotazione definitiva.

- L'intervento vero e proprio avrà luogo in una terza fase, in momento e secondo il piano di lavoro concordato con il nostro cliente.

GP&A Srl - Via Seprio, 2 - 20149 Milano - Tel: 02/45.49.53.73 Fax: 02/45.49.53.74 - Email: info@gpa.it

Il dato personale

L'oggetto di applicazione della legge è quindi il dato personale, inteso come "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, direttamente od indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

La legge distingue poi i dati personali in dati identificativi, dati sensibili e dati giudiziari e per ogni categoria andrà a costruire le norme di tutela più idonee.

Il trattamento dei dati personali

L'ambito di applicazione di questa normativa è quindi regolare, in funzione del diritto alla riservatezza, l'utilizzo, la diffusione dei dati personali, inteso come "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 dati.

A chi è diretto il "Codice di Protezione dei dati personali"

La normativa si rivolge a tutti i soggetti (pubblici e privati) che, in possesso di dati personali possono essere considerati come potenziali soggetti di un trattamento di tali dati lesivo del diritto alla riservatezza ed alla privacy, in particolare:

- liberi professionisti e aziende;
- associazioni e cooperative;
- pubbliche amministrazioni;
- soggetti esteri che trattino i loro dati sul territorio nazionale.

L'elenco riassume rapidamente le categorie di soggetti che devono adottare particolari comportamenti volti a garantire la protezione di informazioni che possono ledere i diritti di terzi:

GP&A Srl - Via Seprio, 2 - 20149 Milano - Tel: 02/45.49.53.73 Fax: 02/45.49.53.74 - Email: info@gpa.it

- clienti e utenti
- fornitori
- dipendenti
- pazienti
- colleghi, soci e associati
- privati cittadini

Come rispettare la normativa…

Non è possibile creare una casistica esauriente di come utilizzare il proprio sistema informativo alla nuova normativa.

Di seguito una serie di spunti, che vuole solo dare ai soggetti sottoposti al rispetto della nuova normativa un'idea generale per comprendere se, ed in che misura, le nuove disposizioni di legge vadano a impattare sul proprio sistema informativo e sulla attuale

È importante notare per esempio come gli adempimenti richiesti a società che trattino dati sensibili o giudiziari siano decisamente più restrittivi rispetto a quanto stabilito dalla legge 675/96.

Il riferimento particolare è rivolto alla necessità di "Notificazione al Garante" per il trattamento dati determinate tipologie di dati.

Altro particolare riferimento è rivolto all'adozione di misure minime di sicurezza volte a garantire la riservatezza degli archivi elettronici, in particolare:

- adeguate procedure di autenticazione informatica;
- procedure di gestione delle credenziali di autenticazione che si rifacciano al principio del "need to know": ogni incaricato ha accesso esclusivamente a quei dati indispensabili per lo svolgimento della propria attività lavorativa;
- aggiornamento periodico di individuazione dell'ambito di intervento e visibilità delle basi dati consentito ai singoli incaricati ed addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione delle apparecchiature, degli strumenti elettronici e dei dati per i casi di accessi non consentiti mediante l'adozione, con aggiornamento periodico di apparecchiature elettroniche e applicativi software idonei a mantenere e garantire livelli di sicurezza di standard accettabili: firewalls hardware e software, applicativi antivirus aggiornati;
- adozione di procedure per predisposizione, il testing e la custodia delle copie di sicurezza per il ripristino della disponibilità dei dati e dei sistemi;
- obbligo di tenuta di un documento programmatico sulla sicurezza aggiornato, da redigere con cadenza annuale (entro il 31 marzo di ogni anno) e da allegare in nota al bilancio di esercizio;

GP&A Srl - Via Seprio, 2 - 20149 Milano - Tel: 02/45.49.53.73 Fax: 02/45.49.53.74 - Email: info@gpa.it

- obbligo di adozione di tecniche di cifratura e/o di codici identificativi per determinate basi dati che possano rivelare lo stato di salute, accertamenti effettuati da organi sanitari, la vita e le abitudini sessuali;
- adozione delle misure di sicurezza per archivi mantenuti senza l'ausilio di strumenti elettronici;
- aggiornamento periodico di individuazione dell'ambito di intervento e visibilità delle basi dati consentito ai singoli incaricati ed addetti alla gestione o alle unità organizzative;
- obbligo di utilizzo di procedure per un'idonea custodia di atti e documenti da parte delle persone incaricate allo svolgimento di attività che comporti rischio per il diritto di terzi alla riservatezza ed alla privacy;
- adozione di procedure per la conservazione di dati o informazioni in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Il nuovo codice raccomanda inoltre ulteriori precauzioni da seguire:

- procedure volte ad impedire la individuazione nominativa dell'utenza in caso di prestazioni sanitarie o adempimenti giuridici;
- l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
- precauzioni idonee a prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni relative a rivelare lo stato di salute, la vita sessuale ed altre abitudini;
- cautele volte ad evitare che prestazioni sanitarie, ivi compresa l'eventuale consegna o lettura della documentazione di anamnesi, avvengano in situazioni di promiscuità derivanti dal tipo di locali prescelti o da qualsiasi altra situazione pregiudizievole;
- la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;
- l'obbligo di sottoporre tramite appositi regolamenti per eventuali categorie di persone non obbligate per legge al segreto professionale a regole di condotta analoghe al segreto professionale, ove esista l'eventualità di una violazione dei diritto tutelato;

GP&A Srl - Via Seprio, 2 - 20149 Milano - Tel: 02/45.49.53.73 Fax: 02/45.49.53.74 - Email: info@gpa.it

Obbligatorietà dell'adeguamento

Il rispetto della nuova normativa è ovviamente obbligatorio ed altrettanto lo sono l'adeguamento dei sistemi informativi, delle procedure e la produzione della documentazione.

La normativa è piuttosto severa: sono previste in caso di inosservanza sanzioni amministrative, civili e penali che variano in funzione del tipo di irregolarità riscontrata e dell'eventuale danno procurato.

Ad esempio, chiunque ometta di adottare le misure minime di sicurezza (artt. 33 – 34 – 35 – 36) è punito con l'arresto sino a due anni e l'ammenda da 10.000 a 50.000 Euro)

Principali scadenze previste dalla nuova normativa:

Il provvedimento è stato approvato il 1° marzo 2005 in via definitiva dal Senato.

Prorogati i termini per la redazione del DPS (Documento Programmatico sulla Sicurezza) che slitta dal **30 giugno 2005 al 31 dicembre 2005**.

Adempimenti periodici

Il codice prevede anche altre scadenze periodiche volte a mantenere l'efficienza delle apparecchiature hardware, software e delle procedure per le quali è prevista l'obbligatorietà.

In particolare deve essere rispettato il seguente calendario:

AGGIORNAMENTO DPSS

- entro il 31 Marzo di ogni anno.

SALVATAGGIO DATI

- aggiornamento con cadenza almeno settimanale.

GP&A Srl - Via Seprio, 2 - 20149 Milano - Tel: 02/45.49.53.73 Fax: 02/45.49.53.74 - Email: info@gpa.it

SCADENZA PASSWORD

- aggiornamento almeno trimestrale.

ANTIVIRUS

- aggiornamento semestrale.

VERIFICA DI EFFICIENZA DELLE APPARECCHIATURE HARDWARE:

- almeno trimestrale.

GP&A Srl - Via Seprio, 2 - 20149 Milano - Tel: 02/45.49.53.73 Fax: 02/45.49.53.74 - Email: info@gpa.it