La Nuova Normativa in materia di Protezione dei Dati Personali, D. Lgs. 30 giugno 2003 n° 196

Prima del 1 Gennaio 2004 i titolari di trattamento dei dati personali si regolavano, per il trattamento dei dati personali, secondo i dettami della legge 675/96 sulla privacy, ma dalla stessa data tutta la normativa precedente che regolava il settore , viene a decadere essendo recepita del tutto dalla nuova normativa (D. Lgs. 196 del 30 Giugno 2003), che è stata ispirata da principi di completezza, chiarezza e semplificazione, facendone di fatto un Testo Unico. Purtroppo per attuare questi ultimi principi non è bastata la nuova normativa perché sui punti risultati poco chiari (e non sono pochi) vanno via via susseguendosi approfondimenti chiarificatori da parte del Garante.

E' importante considerare che il codice della privacy, come legge dello stato, ha una valenza obbligatoria e la sua applicazione da parte dei soggetti obbligati ha una portata rilevante alla stessa stregua della Normativa sulla Sicurezza del Lavoro (626) o sull'autocontrollo HACCP per la somministrazione di alimenti o sulle Normative Antincendio.

Il comportamento degli operatori soggetti alla normativa risulta, in molti casi, disinteressato o superficiale, soprattutto a causa di una non corretta informazione sulla portata normativa del decreto in oggetto, valido erga omnes e su tutti i dati personali trattati a qualsiasi titolo. Persiste una confusione sulla definizione di "Dati Personali", ancor più più se dobbiamo distinguere quelli "comuni" da quelli "sensibili" e quelli di "Dominio Pubblico" da quelli cho non lo sono. Si pensa che i dati interessati nelle aziende siano solo quelli della clientela, trascurando i dati relativi al Personale, ai Fornitori, all'Amministrazione, al Marketing. Non si rilasciano le informative obbligatorie previste dalla legge, non si nominano i soggetti responsabili e incaricati individuati dal codice. Si pensa che l'eventuale adeguamento alla normativa possa comportare solo un adattamento dei sistemi software o la redazione semplicistica di "pseudo" documenti programmatici o semplici informative prese da qualche modulario standard acquistato in libreria o copiato da altri soggetti.

Una cosa risulta fondamentale, qualsiasi riferimento alla normativa sulla privacy comunicato da qualsiasi Titolare del Trattamento ai terzi soggetti con informative (Interessati o Autorità Ispettive) attesta che si è consapevoli dell'esistenza di una normativa specifica che regola la materia e fa presumere che la struttura del Titolare del Trattamento si è adeguata a tutto quanto previsto per la messa in sicurezza dei dati personali (comuni e/o sensibili) e degli obblighi verso gli Interessati e l'Autorità Garante.

Inoltre qualsiasi riferimento alla normativa precedente in essere su qualsiasi documento (come spesso accade sulla legge 675/96), in specie se un contratto o accordo, rende il documento stesso impugnabile. I profili Titolari del trattamento dei dati, Persone Fisiche o Giuridiche, entità nel loro complesso o unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza, sono soggetti all'applicazione della vigente normativa sulla sicurezza dei dati personali. Ciò comporta, per le aziende operanti prima del 31 Dicembre 2003, un adattamento al disposto della nuova normativa soprattutto concernente l'applicazione delle nuove misure minime di sicurezza di cui all'allegato "B" della legge 196/03 ,Disciplinare che ha sostituito il disposto del D. Lgs 318/99. Le nuove imprese dal 1 Gennaio 2004 bisognano di una applicazione totale.

Di seguito si elencano tutte le specifiche della normativa e, in particolare, i soggetti che la legge individua, gli adempimenti, le formalità, lo scadenziario generale, le richieste, i principali adempimenti periodici e il sistema sanzionatorio previsto:

SOGGETTI INDIVIDUATI DALLA LEGGE

I. Titolare del trattamento dei dati;
II. Responsabile del Trattamento;
III. Rappresentante del Titolare nel Territorio Nazionale;
IV. Incaricati per il Trattamento.

ADEMPIMENTI PREVISTI DALLA LEGGE

I. Notificazione;
II. Informativa;
III. Richiesta di Consenso;
IV. Adeguamento alle misure Minime di Sicurezza;
V. Documento Programmatico sulla Sicurezza

Quali le formalità richieste dalla legge 196/03.

I. Notificazione e DPS, al momento chi sono i soggetti obbligati e quali gli adempimenti.

Soggetti obbligati: Per semplificazione tutti i soggetti che trattano dati sensibili , dettagliati all'art 37 della legge 193/03, e/o giudiziari.

Adempimenti: NOTIFICAZIONE da effettuare prima dell'inizio del trattamento dei dati personali da parte del titolare verso il Garante e, visto che il codice ha abrogato la legge precedente, i soggetti obbligati che hanno iniziato il trattamento prima del 1/1/2004, dovevano effettuare (o rieffettuare) la notificazione entro il 30 Aprile 2004 (ora termine prorogato al 30 Giugno 2004). In ogni caso bisogna tenere conto delle autorizzazioni che ogni anno vengono emanate e/o rinnovate dal Garante.

Adempimenti: DPS (Documento Programmatico sulla Sicurezza) da redigere e aggiornare ogni anno a cura del titolare (o del responsabile, se designato) entro il 31 Marzo se si trattano dati sensibili con l'ausilio di apparecchiature elettroniche. Inoltre Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

II. Dati sensibili – giudiziari di cui all'art 37 del D. Lgs. 196/03

In generale si pensa non si trattino dati sensibili e/o giudiziari, ma in realtà si possono facilmente acquisire delle tipologie di dati che vi rientrano, ed in particolare i dati relativi al personale dipendente, parte dei quali rientrano nelle tipologie di cui all'art. 37 del dpr 193/03 . Da ciò consegue che bisogna sempre tenere conto del trattamento di questi tipi di dati, delle dispense autorizzatorie temporanee concesse dal Garante per alcuni adempimenti e dell'obbligo dell'attuazione delle misure minime di sicurezza per questo tipo di trattamento.

III. Misure minime per la sicurezza previste dalla legge 196/03 nel suo allegato "B" (disciplinare tecnico in materia di misure minime di sicurezza) sia in caso di trattamento dei dati con strumenti elettronici che non.

Le misure minime debbono essere previste IN OGNI CASO, sia su trattamento di dati sensibili che non, e sono obbligatorie dal 30 giugno 2005, data prevista per l'adeguamento dei titolari alle misure minime previste dal garante nell'allegato "B" alla legge. In caso di non possesso degli strumenti adeguati previsti dalla legge, è possibile chiedere un rinvio motivato al 31/12/2005 ai fini della scadenza primacitata, ma ciò non preclude una responsabilità del titolare nel caso di perdita o distruzione o diffusione non autorizzata dei dati dal 30 giugno 2005 in poi.

Le misure minime si possono così sintetizzare:

I. Caso trattamento con strumenti elettronici
a. Requisiti hardware e logistiche;
b. Requisiti software;
c. Individuazione dei soggetti (Titolare, Responsabile, Incaricato) e lista degli incaricati;
d. Mansionari per i Soggetti, Autorizzazioni, Autenticazioni, Scadenze, Aggiornamenti, Analisi dei Rischi, loro Formazione;

II. Caso trattamento senza utilizzo di strumenti elettronici
a. Requisiti Logistici;
b. Istruzioni scritte agli incaricati finalizzate al controllo ed alla custodia degli atti e dei documenti, Analisi dei Rischi, loro Formazione;
c. Individuazione dell'ambito del trattamento consentito ai singoli incaricati,
i. suo aggiornamento annuale,
ii. redazione della lista degli incaricati anche per classi omogenee di incarico e dei relativi profili di autorizzazione

Nel caso di Dati Sensibili (In Aggiunta)

III. Caso trattamento con strumenti elettronici.
a. DPS obbligatorio entro il 31 marzo;
b. Notificazione inizio trattamento, e variazioni;
c. Ulteriori misure di sicurezza informatica;
d. Scadenze più ravvicinate per gli adempimenti della sicurezza informatica

IV. Caso trattamento senza utilizzo di strumenti elettronici (In aggiunta)
a. Documenti controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
b. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

SCADENZIARIO GENERALE

Annualmente, aggiornare l'individuazione dell'ambito di trattamento consentito ai singoli incaricati, ove variato, anche parzialmente;
Annualmente, e precisamente entro il 31 marzo di ogni anno, redigere il Documento Programmatico sulla Sicurezza di cui all'art.19, Allegato B (in caso di trattamento di dati sensibili con strumenti elettronici);
Aggiornare con cadenza almeno semestrale gli strumenti elettronici utilizzati al fine di proteggere i dati dal rischio di intrusione e dal rischio derivante da virus informatici (art. 16, Allegato B);
Aggiornare con cadenza almeno annuale (semestrale per il trattamento di dati sensibili) i programmi per computer volti a prevenire la vulnerabilità di strumenti elettronici ed a prevenirne i difetti (art. 17, Allegato B);
Fornire istruzioni organizzative e tecniche affinché il salvataggio dei dati sia effettuato settimanalmente;
Annualmente, programmare interventi di formazione per gli incaricati del trattamento.
Notificazione (art.37):
a) Le notificazioni devono essere effettuate prima dell'inizio del trattamento (qualunque esso sia, manuale o automatizzato), se si rientra in una delle ipotesi previste dall'art. 37 del Codice.
b) Per i trattamenti iniziati prima dell'1 gennaio 2004, le notificazioni devono essere effettuate, in sede di prima applicazione del Codice, entro il 30 Giugno 2004.
Rispettare le autorizzazioni emanate dal Garante per il trattamento dei dati sensibili; esse vengono rinnovate annualmente. Per trattare lecitamente i dati sensibili, infatti, non è sufficiente

ottenere il consenso dell'interessato, ma occorre verificare che il trattamento dei dati sia conforme a quanto indicato dal Garante nelle autorizzazioni, speciali o generali che siano.

RICHIESTE DELL'INTERESSATO

In caso di richiesta da parte dell'interessato, il Titolare deve adoperarsi per rispondere tempestivamente alle richieste dello stesso. In caso di mancata risposta entro quindici giorni dal ricevimento della sua richiesta, l'interessato potrà rivolgersi all'Autorità Giudiziaria o all'Autorità Garante per ottenere soddisfazione dei propri diritti (artt.145 e segg. del Codice).

PRINCIPALI ADEMPIMENTI PERIODICI

Oltre ai principi generali appena enunciati, il D.Lgs. 196/2003 impone una serie di verifiche e controlli da effettuare con cadenza periodica, o per espressa previsione normativa, o perché necessario procedere ad alcune modifiche ogniqualvolta muti uno degli elementi essenziali dell'organizzazione aziendale.

1° gennaio di ogni anno (si tratta degli adempimenti per i quali il Codice prevede una cadenza almeno annuale):

Aggiornare l'individuazione dell'ambito di trattamento consentito ai singoli incaricati, ove variato, anche parzialmente;
Verificare la sussistenza delle condizioni per la conservazione delle autorizzazioni per l'accesso ai dati particolari per gli incaricati;
Fornire istruzioni organizzative e tecniche affinché il salvataggio dei dati sia effettuato settimanalmente;
Programmare interventi di formazione per gli incaricati del trattamento.
Provvedere all'aggiornamento delle "patch" dei programmi per computer, nel caso di trattamento di dati comuni (art. 17, Allegato B);

1°gennaio - 1°luglio di ogni anno (adempimenti a cadenza semestrale):

Aggiornare i software antivirus, per tutti i tipi di dati (art. 16, Allegato B);
Provvedere all'aggiornamento delle "patch" dei programmi per computer, nel caso di trattamento di dati sensibili (art. 17, Allegato B);

31 marzo di ogni anno: Aggiornare il Documento Programmatico sulla Sicurezza.

All'interno del DPS deve essere previsto un PIANO DI FORMAZIONE per i responsabili e gli Incaricati, che dovrà pertanto essere rivisto annualmente. Il piano impone che siano fatte previsioni effettive sui tempi di formazione e sulle strutture che gestiranno tali attività, nell'arco dell'anno. La formazione è programmata al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o introduzione di nuovi significativi strumenti, rilevanti per il trattamento dei dati personali.
Quanto ai Responsabili, questi devono essere scelti tra persone dotate della necessaria esperienza, capacità, affidabilità: è, quindi, opportuno che la loro formazione sia più specifica rispetto a quella data agli incaricati, onde evitare il rischio di nomine invalide.
Inoltre, in tutti i casi che seguono è necessario procedere a verifiche costanti (il legislatore non indica un periodo minimo di revisione, ma punisce dichiarazioni eventualmente difformi dalla realtà):

NOTIFICA

Sarà necessario provvedere alla modifica della notificazione effettuata al Garante tutte le volte in cui cambi uno degli elementi in essa contenuti.

INFORMATIVE

E’ necessario in ogni caso fornire le informative a tutti gli interessati con i quali si hanno relazioni di qualsiasi tipo che comportino l’acquisizione e/o il trattamento dei loro dati personali. Inoltre bisogna distribuire nuove informative, o comunicare i mutamenti intervenuti, tutte le volte in cui cambi uno degli elementi descritti dall’art. 13 del Codice:

a. le finalità e le modalità del trattamento cui sono destinati i dati;
b. la natura obbligatoria o facoltativa del conferimento dei dati;
c. le conseguenze di un eventuale rifiuto di rispondere;
d. i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
e. il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del Titolare.

Non c’è obbligo di modificare l’informativa qualora cambino i Responsabili, che siano stati indicati nell’informativa solo in base alla qualifica rivestita; può anche essere indicato solo il luogo dove è conservato l’elenco completo dei Responsabili del trattamento, ovvero il modo per accedervi. E’ comunque necessario indicare nome e dati di almeno un Responsabile, se nominato.

QUALITA’ DEI DATI

Il Titolare deve curare che il trattamento dei dati avvenga sempre nel rispetto dei principi dettati dall’art.11 del Codice; dunque, occorre verificare costantemente:

a. che i dati siano trattati in modo lecito e secondo correttezza;
b. che siano raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
c. che siano esatti e, se necessario, aggiornati;
d. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e. 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.

CONSENSO

E’ necessario, in generale, procedere alla verifica dell’esistenza del consenso ogniqualvolta il trattamento sia effettuato per scopi diversi da quelli per cui il consenso era stato inizialmente prestato , nonché tutte le volte in cui i dati debbano essere comunicati a soggetti terzi, o diffusi ad un numero di persone indeterminato.

COMUNICAZIONI ALL’INTERESSATO RELATIVE ALLO STATO DI SALUTE

Le comunicazioni all’interessato riguardanti lo stato di salute devono essere effettuate tramite il medico di medicina generale designato dall’interessato o dal Titolare; verificare dunque che tale regola sia sempre rispettata.

SISTEMA SANZIONATORIO

Sono previste, per il non rispetto degli adempimenti e delle formalità dettate dalla legge 196/03, una serie di misure sanzionatorie di tipo amministrativo e penali che possono essere così riassunte