Roma, 19 aprile 2000
Prot. n. 0116/00/E.15.8.
CIRC. N. 16138

Alle Aziende associate

L o r o S e d i

OGGETTO: Tutela della privacy - D.p.r. 28 luglio 1999, n. 318 - Adozione delle misure minime di sicurezza - Proroga del termine - Linee guida per la stesura del documento programmatico sulla sicurezza.

La Commissione Giustizia della Camera dei Deputati, convocata in sede legislativa, ha approvato "in linea di principio" il d.d.l. n. 6885 che proroga al 31 dicembre 2000 il termine per l'adozione delle misure minime di sicurezza di cui al d.p.r. n. 318/99, originariamente fissato al 29 marzo 2000.

Il testo approvato, che ha modificato integralmente quello trasmesso dal Senato (d.d.l. S-4531), per il quale è ora richiesto il parere della Commissione Affari Costituzionali nonché l'esame in terza lettura da parte del Senato così recita:

"Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'art. 15 della legge 31 dicembre 1996, n. 675"

Art. 1

1. In sede di prima applicazione della disciplina contenuta nell'articolo 15 della legge 31 dicembre 1996, n. 675, le misure minime di sicurezza di cui al d.p.r. 28 luglio 1999, n. 318, possono essere adottate entro il 31 dicembre 2000 dai soggetti che si avvalgono della facoltà regolata dal presente articolo.
2. I soggetti che hanno avviato l'adeguamento delle procedure minime di trattamento di dati personali alle prescrizioni in materia di sicurezza contenute nell'articolo 15, commi 1 e 2, della legge 31 dicembre 1996, n. 675, possono completarlo entro il 31 dicembre 2000 qualora documentino per iscritto le particolari esigenze tecniche ed

organizzative che rendono necessario avvalersi di un termine più ampio di quello previsto ai sensi dell'art. 41, comma 3, della medesima legge.
3. Il documento di cui al comma 2 deve essere redatto entro il 30 aprile 2000 con atto avente data certa e deve contenere una esposizione sintetica delle informazioni necessarie, da cui risultino:
a) gli accorgimenti già adottati e gli elementi che caratterizzano il programma di adeguamento, nonchè le singole fasi in cui esso è eventualmente ripartito;
b) le linee-guida previste per dare piena attuazione alle misure minime di sicurezza, la cui inosservanza è sanzionata ai sensi dell'art 36 della cittata legge, nonchè alle più ampie misure di sicurezza previste al comma 1 dell'articolo 15 della legge 31 dicembre 1996, n. 675.

Art. 2

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale."

Peraltro va detto che l'Ufficio del Garante per la tutela dei dati personali ha assicurato, su sollecitazione di Confindustria, che il termine del 20 aprile, utile ai fini della presentazione della documentazione necessaria per ottenere la proroga, sarà spostato al 31 maggio p.v..

La stessa Autorità Garante per la privacy ha espresso parere favorevole alle linee guida per la stesura del Documento programmatico sulla sicurezza - previsto dall'art. 6, d.p.r. n. 318/99, cit. - presentate da Confindustria.

Il documento (che trasmettiamo in allegato), redatto in collaborazione con IBM, non può essere considerato esaustivo di ogni misura di sicurezza applicabile ai singoli dati e trattamenti, atteso che le misure di sicurezza possono variare non solo nel tempo ma anche in funzione di diversi fattori. Tra questi, ad esempio, quello legato alle conoscenze acquisite in base al progresso tecnico, che variano al variare delle esigenze tecniche e organizzative che ciascun titolare ha all'interno della propria struttura.

Cordiali saluti.

Nicola De Marinis
DIRETTORE
AREA RELAZIONI INDUSTRIALI

All.
RT/it

Linee guida per la stesura del documento programmatico della sicurezza *ex* art. 6, d.p.r. n. 318/99, contente il *"Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675".*

La normativa

L'art. 6, d.p.r. n. 318/99, sul "*documento programmatico sulla sicurezza"* dispone che:

"1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 (sui dati sensibili e giudiziari) della legge effettuato mediante gli elaboratori indicati nell'articolo 3, comma 1, lettera b) (cioè attraverso elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico), deve essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:

a) i *criteri tecnici e 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 locali medesimi;
b) i *criteri* e le *procedure* per assicurare *l'integrità dei dati*;
c) i *criteri* e le *procedure* per la *sicurezza delle trasmissioni dei dati*, ivi compresi quelli per le restrizioni di accesso per via telematica;
d) l'elaborazione di un *piano di formazione per* rendere edotti *gli incaricati del trattamento* dei rischi individuati e dei modi per prevenire danni.

2. L'efficacia delle misure di sicurezza adottate ai sensi del comma 1, deve essere oggetto di *controlli periodici, da eseguirsi con cadenza almeno annuale*."

Nella sostanza, ciò che occorrerà fare sarà:

A - *Analisi dell'esistente:*

a/1 - Analisi dei trattamenti

- individuare i trattamenti di dati personali presenti in azienda (saranno, ovviamente, tutti quelli ancora attivi e già notificati al Garante. Nel caso in cui ne siano sorti dei nuovi,

ricordiamo che questi dovranno essere immediatamente notificati. E' da considerarsi "nuovo trattamento" l'inserimento di nuove categorie di dati in una banca/trattamento dati già attivata, ovvero il compimento di nuove operazioni di trattamento (registrazione, selezione, comunicazione, ecc..) nel quadro di una attività di trattamento già in atto. Deve trattarsi, in sostanza, dell'inizio di una attività del tutto nuova;
- individuare la natura dei dati trattati (sensibili, giudiziari, comuni);
- individuare l'incaricato del trattamento;
- individuare l'ambito di comunicazione.

a/2- Analisi delle aree e dei locali

- individuare, per ciascun trattamento, le aree ed i locali in cui è conservato.

a/3 - Analisi degli strumenti elettronici o automatizzati utilizzati per il trattamento

- PC;
- elaboratori portatili;
- server;
- centralino con registrazione delle chiamate;
- telecamere a circuito chiuso con conservazione dei filmati;
- rilevatori di presenze;
- altro.

a/4 - Analisi degli strumenti non elettronici o comunque non automatizzati utilizzati per il trattamento

- raccolte cartacee;
- raccolte di fotografie;
- raccolte di slides;
- raccolte di fiches;
- raccolte di nastri magnetici (ad esempio, video, audio);
- altro.

a/5 - Analisi dei rischi

Procedere per ciascun dato, con riferimento:
- alle aree ed ai locali in cui sono conservati;
- agli strumenti utilizzati;
- all'ambito di comunicazione;
- alla individuazione ed analisi dei relativi rischi, anche accidentali.

a/6 - Distribuzione dei compiti e delle responsabilità

- nomina del responsabile del trattamento (in ordine ai compiti ed alle responsabilità attribuitegli dal titolare del trattamento);
- nomina degli incaricati del trattamento (in ordine alle istruzioni ricevute dal responsabile e/o dal titolare del trattamento);
- nomina degli incaricati autorizzati del trattamento (in ordine alle autorizzazioni e istruzioni ricevute dal responsabile e/o dal titolare del trattamento);
- nomina dei custodi delle parole chiave (in ordine alle istruzioni ricevute dal responsabile e/o dal titolare del trattamento);
- nomina dell'amministratore di sistema (in ordine all'incarico e alle responsabilità attribuitegli dal titolare del trattamento);
- altro.

B - Individuazione delle misure di sicurezza

Con riferimento ai criteri e alle procedure, tecniche e organizzative, per assicurare:

- la protezione delle aree e dei locali in cui sono conservati i dati personali interessati dalle misure di sicurezza;
- il controllo sull'accesso nei predetti locali delle persone autorizzate;
- la integrità dei dati;
- la trasmissione dei dati, ivi comprese quelle da adottarsi per le restrizioni di accesso per via telematica.

C - Elaborazione di un piano di formazione

Per rendere noti agli incaricati del trattamento i rischi individuati e le modalità per prevenire relativi danni.

D - Adozione di controlli periodici

Da effettuarsi, con cadenza almeno annuale, sul contenuto del documento programmatico sulla sicurezza e sulle misure di sicurezza adottate.

* * *

Quanto sopra è stato previsto dal d.p.r. n. 318/99 con riferimento esclusivo ai trattamenti di dati sensibili e giudiziari effettuati mediante elaboratori accessibili in rete disponibile al

pubblico. Pertanto, il documento sulla sicurezza potrebbe limitarsi a *contenere unicamente le misure **minime** di sicurezza approntate con riferimento a tali trattamenti*.

Nonostante ciò, suggeriamo di provvedere ad elencare *non solo le misure minime adottate* ex *d.p.r. n. 318/99, cit.* (cioè quelle richiamate al comma 2, dell'art. 15, l. n. 675/96), *ma anche quelle massime adottate* ex *art. 15, comma 1, n. 675/96, cit.* che devono necessariamente essere sottoposte ad aggiornamenti periodici tali da permettere che i dati personali oggetto di trattamento (effettuato sia attraverso strumenti elettronici o automatizzati che attraverso raccolte cartacee) siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati (sensibili o comuni) e alle specifiche caratteristiche del trattamento. Ciò al fine di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (così art. 15, comma 1, l. n. 675/96).

Quanto sopra significa che *sarebbe opportuno estendere il documento programmatico sulla sicurezza per comprendervi anche i dati comuni nonché le misure di sicurezza minime e massime adottate con riferimento ai trattamenti cartacei*. Ciò consentirebbe all'azienda (comunque tenuta a rispettare tali misure) di avere un quadro completo e sempre aggiornato di tutte le misure di sicurezza adottate.

Merita sottolineare che, anche secondo quanto anche dichiarato dal Dott. Buttarelli (Segretario Generale dell'Aurorità garante per la privacy) in occasione del seminario sulle misure minime di sicurezza organizzato da Confindustria il 29 novembre 1999, il documento programmatico costituisce esso stesso una misura minima di sicurezza. Chi non lo redige o non lo aggiorna o non ne verifica l'efficacia è punibile *ex* art. 36, l. n. 675/96, anche se la norma non punisce penalmente chi non attua tutte le misure previste nel documento programmatico perché, se così fosse, si avrebbe un'alterazione del concetto di misura minima.

La l. n. 675/96 dispone inoltre che le misure minime di sicurezza di cui al Regolamento *ex* d.p.r. n. 318/99, saranno adeguate con cadenza almeno biennale attraverso l'adozione di successivi Regolamenti che terranno conto "dell'evoluzione tecnica del settore e dell'esperienza maturata" (cfr. art. 15, comma 3).

* * *

Premesso quanto sopra, provvediamo a fornirVi qui di seguito le linee guida utili alla stesura del predetto documento (riassunte nel prospetto all. 2) che tengono conto anche delle opportunità sopra ricordate di elaborare un documento programmatico "allargato".

A - La legge n. 675/96 richiede esplicitamente che i dati personali vengano protetti da specifici rischi che possono essere causati da numerose minacce.

Minacce:

- alterazione di programmi e dati ;
- disastri naturali (incendio, allagamento…);
- sabotaggio;
- divulgazione/comunicazione non autorizzata;
- virus in rete;
- utilizzo indebito, violazioni al sistema da parte di hackers;
- duplicazione e diffusione a scopo di lucro e per danneggiare l'immagine;
- sottrazione/furto;
- danneggiamenti alle risorse informatiche;
- errori umani per imperizia, negligenza o imprudenza;
- altro.

Rischi:

- distruzione/perdita (anche accidentale);
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta.

Conseguenze:

- sanzioni civili;
- sanzioni penali;
- perdite economiche/finanziarie;
- perdita d'immagine;
- costi gestionali;
- responsabilità contrattuali .

B - Per capire a quali rischi le informazioni sono esposte, è necessario individuare e selezionare i dati, rilevare dove sono contenuti, come circolano all'interno e verso l'esterno, come sono trattati….

Selezione dei dati:

- dati personali sensibili;
- dati personali giudiziari;
- dati personali comuni.

Rilevazione dei supporti:

- personal computer;
- portatile;
- sistema centrale;
- server;
- lan;
- dischetto;
- nastro magnetico (es. video, audio);
- archivio (cartaceo, di fotografie, fiches, slides, diapositive…)*;*
- *altro.*

Soggetti che trattano i dati

- identificare i soggetti ai quali è consentito l'accesso ai dati e fornire relative istruzioni per l'utilizzo;
- altro.

Ambito di comunicazione dei dati

- interno;
- esterno;
- altro.

Evidenza del rischio in relazione a:

1) tipo dato(comune, sensibile, giudiziario);
2) soggetti che li trattano;
3) ambito di comunicazione ;
4) supporto (pc, lan, archivio…);
5) locale/area dove sono custoditi i supporti (es. locali ced);
6) modalità trattamento (elettronico o automatizzato/non elettronico e comunque neppure automatizzato).

C - Individuazione delle misure idonee: alcuni suggerimenti di ordine normativo e tecnico per la protezione dei dati personali trattati con strumenti elettronici

Protezione fisica del server

- locali chiusi;
- accesso ai locali :
  - controllato;
  - solo alle persone autorizzate;
  - altro;
- sistemi di allarme;
- dispositivi antincendio;
- continuità elettrica;
- dispositivi antintrusione (specifici o generali);
- servizio di vigilanza interno e/o esterno ;
- climatizzazione dei locali.

Protezione logica del server

- sistema operativo:
  - aggiornato con ultime patch;
  - protetto (eliminare servizi non necessari);
  - antivirus/antintrusione aggiornato;
  - altro;
- identificazione e autenticazione:
  - userid e password (pw robusta, criptata);
  - altro;
- controllo accessi:
  - utenti autorizzati;
  - altro;
- protezione dati personali:
  - accessi selettivi;
  - crittografia;
  - altro;
- log degli accessi e delle attività.

Protezione personal computers portatili

- non dovrebbero esservi archiviati o elaborati dati personali (soprattutto sensibili);
- se necessaria la memorizzazione su hard disk: utilizzo di un prodotto di crittografia;
- custodia fisica: adozione di tutte le misure necessarie (in viaggio, auto, albergo…);
- produzione di backup e loro custodia;
- installazione prodotto antivirus e pronto aggiornamento;
- password di accensione.

Protezione stazioni di lavoro

- controllo sequenza IPL:
  - solo da disco fisso;
  - schermatura disco fisso;
  - altro;
- protezione sistema operativo:
  - versione aggiornata/corretta;
  - modifiche impedite;
  - altro;
- protezione programmi applicativi:
  - evitare esecuzione non abilitata;
  - altro;
- controllo accessi e protezione informazioni:
  - utilizzo chiave fisica (hw);
  - utilizzo chiave logica (sw);
  - altro;
- crittografia;
- registrazione delle attività;
- distribuzione/aggiornamento programmi antivirus;
- nomina custode delle parole chiave.

Protezione rete e lan

- apparecchiature installate in aree chiuse e protette (server, gateways, bridge, router);
- cavi di connessione protetti e sotto controllo;
- armadi e/o contenitori delle apparecchiature di collegamento chiusi a chiave;
- server e unità di controllo locale:
  - locali chiusi;
  - unico amministratore;
  - gestione locale;
  - controllo centrale;
  - altro;
- logica elaborativa locale:
  - distribuita centralmente;
  - controllo centrale;
  - antivirus attivi;
  - protetta localmente (per stazioni di lavoro);
  - server con backup automatico;
  - altro;
- dati sensibili criptati in fase di trasmissione:

- protocollo di sicurezza-ssl (secure socket layer);
- rete virtuale crittografata-vp (virtual private network);
- prodotto hw di crittografia: tool box;
- sw di crittografia;
- altro;

➢ accessi controllati:
- verifiche a più live;
- validazione centrale (identificazione, autenticazione);
- altro;

➢ rilevazione delle intrusioni.

Backup e disaster recovery

➢ dati personali (sensibili, giudiziari e comuni) salvati periodicamente:
- nastri;
- dischetti;
- altro;

➢ salvataggi:
- custoditi in altro luogo;
- protetti (armadi ignifughi/blindati);
- altro;

➢ test periodico di recovery:

➢ definizione e aggioranamento piano disaster recovery.

D - Trattamento dei dati personali effettuato con strumenti non elettronici e comunque non automatizzati (dati sensibili, giudiziari,comuni)

Protezione accesso aree/locali con dati personali

➢ locali chiusi;

➢ accesso agli archivi:
- selezionato;
- identificazione e registrazione dei soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi;
- altro;

➢ sistemi di allarme nei locali;

➢ dispositivi antincendi nei locali;

➢ continuità elettrica;

➢ utilizzo di armadi o classificatori muniti di chiusura, ignifughi e blindati;

➢ nomina di custode delle chiavi di accesso;

➢ climatizzazione dei locali;

- sistema di vigilanza interno e/o esterno;
- dispositivi antintrusione (specifici o generali).

Accesso ai dati personali

- solo alle persone autorizzate;
- obbligo della restituzione degli atti e documenti al termine delle operazioni;
- fino alla restituzione: conservazione in contenitori muniti di chiusura, ignifughi e blindati, …;
- nomina di un custode delle chiavi di accesso.

Anche per la conservazione e consultazione delle riproduzioni (es. fotocopie, fiches…) valgono le regole di cui sopra.

E - Adozione di un piano di formazione

Per illustrare agli incaricati e, se ritenuto opportuno, anche ai responsabili del trattamento (i quali, *ex* art. 8, l. n. 675/96 sono anch'essi responsabili, al pari del titolare del trattamento, dell'adozione delle misure di sicurezza sui dati personali), i rischi individuati e i modi per prevenire i danni.

Al riguardo, occorrerà:
- adottare un piano formativo;
- individuare i destinatari;
- conservare la documentazione distribuita;
- fissare la periodicità degli incontri.

_____

Questo documento non è e non può essere considerato esaustivo di ogni misura di sicurezza applicabile ai singoli trattamenti di dati personali, atteso che le misure di sicurezza possono variare non solo nel tempo ma anche in funzione di molteplici fattori, tra i quali determinante risulta essere quello legato alle conoscenze acquisite in base al progresso tecnico, conoscenze che, a loro volta, variano al variare delle diverse esigenze tecniche ed organizzative che ciascun titolare ha all'interno della propria struttura.

Allegato 2

TUTELA DELLA PRIVACY

Prospetto delle linee guida sulle misure di sicurezza adottate e da adottare al…. [data]

NOME *TRATTAMENTO O BANCA DATI*	*DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'*	NATURA DEI DATI *PERSONALI TRATTATI*	FINALITA' DEL *TRATTAMENTO*	CATEGORIE SOGGETTI CUI SI RIFERISCONO *I DATI*	*AMBITO DI COMUNICAZIONE E DIFFUSIONE*	MODALITA' DEL TRATTAMENTO	LOCALE DOVE SO CUSTOD *SUPPOR*
	♦ Responsabilità del trattamento; ♦ Amministratore di sistema; ♦ Custode parole chiave; ♦ Incarichi autorizzati; ♦ Altro; (le attribuzioni sono, ovviamente, quelle risultanti da atto scritto)	♦ Sensibili; ♦ Giudiziari; ♦ Comuni;	(quelle dichiarate al Garante attraverso la notificazione)	♦ Dipendenti; ♦ Clienti; ♦ Associati; ♦ Altro;		♦ Con strumenti elettronici; ♦ Con strumenti automatizzati; ♦ Altro;	♦ Loca ♦ Area ♦ Altro

ANALISI DEI RISCHI	*MISURE DI SICUREZZA SU AREE E LOCALI*		MISURE DI SICUREZZA SUI DATI		MISURE DI SICUREZZA PER LA TRASMISSIONE DEI DATI		PIANO DI FORMAZION	
♦ Distruzione;	*ADOTTATE*	*DA ADOTTARE*	*ADOTTATE*	*DA ADOTTARE*	*ADOTTATE*	*DA ADOTTARE*	*REALIZZATE*	*REA*

♦ Perdita; ♦ Accesso non autorizzato; ♦ Trattamento non consentito; ♦ Trattamento non conforme alle finalità della raccolta;	- Tecniche; - Organizzative; Procedure per il controllo delle persone che hanno accesso alle aree ed ai locali	- Tecniche; - Organizzative;	- Tipologia; - Procedura; Procedure per il controllo delle persone che hanno accesso ai dati	- Tipologia; - Procedura;	- Tipologia; - Procedura;	- Tipologia; - Procedura;	♦ Soggetti interessati; ♦ Contenuti; ♦ Documentazione distriibuita;	