Confederazione Generale Italiana
dei Trasporti e della Logistica
via Panama 62 - 00198 Roma - tel. 06.8559151 - fax 06.8415576
e-mail: confetra@tin.it - http://www.confetra.com

Roma, 18 ottobre 1999

CIRCOLARE N. 143/1999
OGGETTO: ORDINE PUBBLICO – "*PRIVACY*" – MISURE MINIME DI SICUREZZA – REGOLAMENTO 28.7.1999, N.318, SU G.U. N.216 DEL 14.9.1999.

Come e' noto, la legge 675/96 sulla tutela della privacy, passata la fase di prima applicazione, non ha comportato aggravi particolari all'operativita' delle imprese.
Peraltro con il regolamento indicato in oggetto, attuativo dell'articolo 15 della legge, e' stato introdotto l'obbligo per tutte le imprese di adottare alcune misure minime di sicurezza al fine di evitare il rischio di accesso non autorizzato all'archivio dati.
La protezione sulla custodia dei dati personali deve applicarsi a tutte le fattispecie di dati, sia quelli che devono essere gestiti previo consenso dell'interessato (i cosiddetti dati "*sensibili*" come quelli che rientrano nell'ambito dell'elaborazione delle paghe, quali l'appartenenza del dipendente al sindacato, il suo credo politico e religioso, le notizie sulla sua salute), sia quelli che possono essere gestiti liberamente (es. elenchi clienti e fornitori, mailing list, rubriche, ecc.).
Le misure di sicurezza da adottare sono diverse a seconda che il trattamento dei dati avvenga con computer autonomi, ovvero con computer collegati in rete tra di loro. Si rammenta che ai sensi della legge 675/96 per "*trattamento*" si intende qualsiasi operazione svolta sui dati personali (registrazione, organizzazione, elaborazione, modificazione, ecc.).
Per quanto concerne i trattamenti con computer autonomi (art.2), e' stato previsto l'obbligo di introdurre nel programma informatico una **parola-chiave** per l'accesso ai dati; ovviamente tale parola chiave deve essere a conoscenza solo dei soggetti che effettuano materialmente il trattamento.
Per quanto concerne i trattamenti con computer collegati in rete (art.3), nel caso di trattamenti effettuati con piu' computer collegati tra loro, oltre alla parola chiave il programma informatico deve richiedere anche un apposito **codice identificativo** per consentire l'accesso ai dati; qualora il trattamento riguardi i dati "*sensibili*", inoltre, il titolare dovra' formalmente autorizzare l'incaricato ed individuare il computer abilitato alle varie operazioni.
Si sottolinea che, come per tutte le violazioni che riguardano la legge sulla privacy, anche per l'omissione delle misure di sicurezza e' prevista come pena la **reclusione**.

Per riferimenti confronta circ.re conf.le n.192/98

FINE TESTO CIRCOLARE CONFETRA

G.U. N. 216 DEL 14 09 1999 (fonte Guritel)
DECRETO DEL PRESIDENTE DELLA REPUBBLICA 28 luglio 1999, n. 318.
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.
Capo I
PRINCIPI GENERALI
Art. 1.
Definizioni
1. Ai fini del presente regolamento si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata legge. Ai medesimi fini si intendono per:
a) "misure minime": il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'articolo 15, comma 1, della legge;
b) "strumenti": i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;
c) "amministratori di sistema": i soggetti cui e' conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.
Capo II
TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI.
Sezione I
Trattamento dei dati personali effettuato mediante elaboratori non accessibili da altri elaboratori o terminali.
Art. 2.
Individuazione degli incaricati
1. Salvo quanto previsto dall'articolo 8, se il trattamento dei dati personali e' effettuato per fini diversi da quelli di cui all'articolo 3 della legge mediante elaboratori non accessibili da altri elaboratori o terminali, devono essere adottate, anteriormente all'inizio del trattamento, le seguenti misure:
a) prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore,

consentirne l'autonoma sostituzione, previa comunicazione ai soggetti preposti ai sensi della lettera b);
b) individuare per iscritto, quando vi e' piu' di un incaricato del trattamento e sono in uso piu' parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime.

Sezione II

Trattamento dei dati personali effettuato mediante elaboratori accessibili in rete

Art. 3.

Classificazione

1. Ai fini della presente sezione gli elaboratori accessibili in rete impiegati nel trattamento dei dati personali sono distinti in:
a) elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico;
b) elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico.

Art. 4. Codici identificativi e protezione degli elaboratori

1. Nel caso di trattamenti effettuati con gli elaboratori di cui all'articolo 3, oltre a quanto previsto dall'articolo 2 devono essere adottate le seguenti misure:
a) a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non puo', neppure in tempi diversi, essere assegnato a persone diverse;
b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualita' che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.
2. Le disposizioni di cui al comma 1, lettere a) e b), non si applicano ai trattamenti dei dati personali di cui e' consentita la diffusione.

Art. 5.

Accesso ai dati particolari

1. Per il trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato ai sensi dell'articolo 3, l'accesso per effettuare le operazioni di trattamento e' determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Se il trattamento e' effettuato ai sensi dell'articolo 3, comma 1, lettera b), sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico.
2. L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali e' possibile accedere per effettuare operazioni di trattamento.
3. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, e' verificata la sussistenza delle condizioni per la loro conservazione.
4. L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza e' necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
5. La validita' delle richieste di accesso ai dati personali e' verificata prima di consentire l'accesso stesso.
6. Non e' consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.
7. Le disposizioni di cui ai commi da l a 6 non si applicano al trattamento dei dati personali di cui e' consentita la diffusione.

Art. 6.

Documento programmatico sulla sicurezza

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato mediante gli elaboratori indicati nell'articolo 3, comma l, lettera b), 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 responsabilita' 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 nonche' le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
b) i criteri e le procedure per assicurare l'integrita' 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.

Art. 7.

Reimpiego dei supporti di memorizzazione

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato con gli strumenti di cui all'articolo 3, i supporti gia' utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

Sezione III

Trattamento dei dati personali effettuato per fini esclusivamente personali

Art. 8.

Parola chiave

1. Ai sensi dell'articolo 3 della legge, il trattamento per fini esclusivamente personali dei dati di cui agli articoli 22 e 24 della legge, effettuato con elaboratori stabilmente accessibili da altri elaboratori, e' soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche di dati.

Capo III

TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI.

Art. 9.

Trattamento di dati personali

1. Nel caso di trattamento di dati personali per fini diversi da quelli dell'articolo 3 della legge, effettuato, con strumenti diversi da quelli previsti dal capo II, sono osservate le seguenti modalita':

a) nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli articoli 8, comma 5, e 19 della legge, il titolare o, se designato, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;

b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.

2. Nel caso di trattamento di dati di cui agli articoli 22 e 24 della legge, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalita':

a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura;

b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

Art. 10.

Conservazione della documentazione relativa al trattamento

1. I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali di cui agli articoli 22 e 24 della legge devono essere conservati e custoditi con le modalita' di cui all'articolo 9.

Il presente decreto, munito del sigillo dello Stato, sara' inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addi' 28 luglio 1999

CIAMPI

D'Alema, Presidente del Consiglio dei Ministri

Diliberto, Ministro di grazia e giustizia