CFI – COOPERAZIONE FINANZA IMPRESA

REGOLAMENTO INTERNO AZIENDALE
VALIDO DAL 01 GENNAIO 2013

A) _REGOLAMENTAZIONE PRESENZE E TRASFERTE

A 1 - orario di lavoro
A 2 - lavoro supplementare e straordinario
A 3 - ferie
A 4 – permessi/assenze per malattia
A 5 - missioni, trasferte e rimborsi spese

B) DISCIPLINA – C.C.N.L. Commercio/Terziario

C) SICUREZZA

D) PRIVACY

E) GESTIONE COMPUTERS AZIENDALI, PROGRAMMI, INTERNET

v.1.1

A) REGOLAMENTAZIONE PRESENZE E TRASFERTE

A 1 – ORARIO DI LAVORO

Premesso che tutto il personale dipendente è tenuto al rispetto dell'orario di lavoro, si comunica che lo stesso si svolge dal lunedì al giovedì dalle ore 09.00 alle ore 18.00 e per la giornata del venerdì dalle 09.00 alle 16.45, con pausa per il pranzo dalle ore 13.00 alle ore 13.45, dal lunedì al venerdì.
E' prevista la flessibilità dell'orario di lavoro, con ingresso tra le ore 09,00 e le ore 09,30 ed uscita, tra le ore 18,00 e le ore 18,30, con pausa pranzo tra le ore 13.00/13.15 e le 13.15/14.00.
Al fine di garantire la funzionalità degli Uffici, l'Ammistrazione e la Segreteria assicureranno la presenza di un addetto che garantisca l'apertura degli Uffici alle ore 09,00.
Tutto il personale dipendente è inoltre tenuto al rispetto delle formalità previste dall'azienda per il controllo delle presenze. Resta inteso che è vietato abbandonare il posto di lavoro, se non preventivamente autorizzati, prima del termine dell'orario di lavoro sopra descritto.

A 1.1 – In riferimento all'orario di lavoro, è consentito l'ingresso negli uffici prima delle ore 09,00 esclusivamente al personale dipendente autorizzato per particolari esigenze personali.

A 1.2 – Sempre in riferimento all'orario di lavoro, si rammenta che il ritardo nell'inizio del lavoro è ammesso soltanto eccezionalmente per comprovate ragioni. Il susseguirsi di più ritardi comporta l'applicazione della sanzione dell'ammonizione scritta.

A 1.3 – I minuti di ritardo, non oltre 30 per ciascuna giornata lavorativa, devono esser recuperati entro la fine della settimana successiva e comunque entro la fine di ciascun mese.
I ritardi, eccezionalmente non compensati, si sommano tra loro, nel mese, e vengono stornati dal monte permessi.
Nel caso in cui non vi sia capienza nel monte permessi (100 ore), i ritardi maturati dal dipendente vengono stornati dalla retribuzione mensile.

A 1.4 – Viene riconosciuto ai dipendenti 1 buono pasto del valore di € 8,00 per ogni giornata lavorativa effettuata all'interno della sede aziendale. Tale benefit, che matura dopo 4 ore lavorative, non è riconosciuto al personale in missione o trasferta in quanto viene effettuato il rimborso a piè di lista.

A 2 – LAVORO SUPPLEMENTARE E STRAORDINARIO

A 2.1 – Non è ammesso il prolungamento del proprio orario di lavoro (lavoro supplementare o straordinario) senza che lo stesso sia stato preventivamente concordato con l'azienda e da quest'ultima autorizzato e decorre successivamente ai primi 30 minuti oltre l'orario normale di lavoro. Il dettaglio delle ore effettuate (supplementari e/o straordinarie) deve essere presentato in segreteria, previo visto del capo servizio, (in caso di trasferta allegato alla richiesta di rimborso) nel giorno immediatamente successivo a quello in cui sono state effettuate le prestazioni orarie supplementari e/o straordinarie.

A 2.2 – Il dipendente può chiedere di trasformare ogni ora di straordinario in altrettante ore di riposo compensativo che però non potrà essere usufruito il giorno successivo allo svolgimento della prestazione straordinaria. La richiesta deve essere presentata entro il mese successivo a quello in cui è stata effettuata la prestazione di lavoro straordinario.

Viceversa, se il lavoratore dichiara nel corso del mese in cui viene effettuata la prestazione di lavoro straordinario di volere il pagamento, questo sarà effettuato normalmente in base ai valori previsti dal C.C.N.L..
In ogni caso, se il lavoratore non dichiara entro il mese successivo a quello in cui è stata effettuata la prestazione di lavoro straordinario, di volere il riposo compensativo, le ore di straordinario effettuate saranno retribuite nel periodo di paga successivo.
L'istituto dei riposi compensativi è interamente regolato dal C.C.N.L..
Tuttavia, in deroga a tale meccanismo, al lavoratore sarà concessa la facoltà di chiedere i riposi compensativi anche con riferimento alle prime 80 ore annue di lavoro straordinario prestato.

A 2.3 – La giornata del sabato è considerata non lavorativa e pertanto, nel caso di festività, non dà diritto ad erogazione di indennità, così come, nel caso di straordinari effettuati in tale giornata, la maggiorazione sarà quella prevista dal C.C.N.L..

A 3 – FERIE
La richiesta di fruizione di giorni di ferie deve sempre essere preventivamente autorizzata dall'azienda, compatibilmente con le esigenze tecnico–produttive ed organizzative dell'azienda stessa. La richiesta deve essere presentata in segreteria con un anticipo di almeno 48 ore rispetto all'inizio del periodo feriale medesimo.

A 3.1 – Premesso che ogni anno l'azienda effettua un periodo di chiusura dei propri uffici nelle due settimane centrali del mese di agosto e che durante tale periodo è ferma ogni attività aziendale, le richieste delle rimanenti giornate di ferie a disposizione di ogni dipendente dovranno tenere conto di tale fatto e della esigenza di buon funzionamento degli uffici.

A 3.2 – Sempre in relazione alle ferie, si specifica che la richiesta stessa di giorni di ferie, deve sempre tener conto della necessità aziendale di garantire in ogni momento la presenza di almeno un dipendente in ogni ufficio. A tal fine, ogni dipendente è tenuto a presentare il proprio personale piano ferie; il responsabile di ogni ufficio, dopo aver raccolto i singoli piani dei dipendenti, redigerà il piano ferie dell' ufficio che andrà consegnato entro il termine del 31 maggio di ogni anno.

A 4 – PERMESSI
A 4.1 – La richiesta di fruizione di ore di permesso deve essere preventivamente vistata e autorizzata dal capo servizio ed autorizzata dall'azienda nel caso dei responsabili di funzione, compatibilmente con le esigenze tecnico-produttive ed organizzative dell'azienda. Tali permessi possono essere personali, per visita medica o per malattia.
I permessi a disposizione retribuiti dall'azienda ammontano a 100 ore annuali (12 ore oltre le 88 ore previste dal CCNL) e possono essere frazionati a partire da 1 (una) ora. Le richieste di ore di permesso devono essere presentate in segreteria almeno 24 ore prima dell'inizio delle stesse.
Per ciò che concerne i permessi per visite mediche o accertamenti diagnostici medici si conferma il trattamento fino ad ora adottato dall'azienda nel limite di 14 ore complessive annuali. Le ore eccedenti saranno considerate permessi retribuiti ordinari. I dipendenti dovranno esibire in originale apposita certificazione medica attestante l'evento. In caso di mancata produzione della certificazione medesima, tale permesso sarà considerato un normale permesso retribuito.

A 4.2 – Si rammenta che, oltre alle ore di permesso previste dal C.C.N.L., l'azienda riconosce ulteriori permessi riconducibili alla normativa vigente sui congedi parentali.

A 4.3 – Assenze per malattia - In parziale deroga a quanto disposto all'articolo n. 176 del vigente CCNL del Commercio, l'azienda integra per tutto il personale, per l'intero periodo di comporto, le indennità di malattia a carico INPS, nella misura del 100% anche nel periodo in cui è previsto il limite al 75% (tra il 4° ed il 20° giorno di un evento di malattia).
In tal modo, fatta salva l'applicazione dell'istituto della "lordizzazione delle integrazioni", sarà garantito ad ogni Lavoratore il trattamento economico a questi riservato senza alcun pregiudizio.

A 5 – MISSIONI, TRASFERTE E RIMBORSI SPESE
A 5.1 – Le missioni o trasferte dei dipendenti devono essere preventivamente autorizzate dal caposervizio e/o dall'azienda. Il dipendente ha l'onere di preparare l'autorizzazione alla missione o trasferta, indicando il luogo di destinazione nonché la motivazione della stessa, far autorizzare la richiesta al caposervizio e consegnare il tutto in segreteria per l'annotazione sul riepilogo mensile delle presenze.
La segreteria provvederà ad effettuare tutte le prenotazioni.

A 5.2 – Durante la missione e la trasferta, la prestazione di lavoro eccedente il normale orario di lavoro, sarà compensata come lavoro straordinario soltanto se espressamente prevista nell'autorizzazione alla trasferta.
La prestazione di lavoro eccedente il normale orario di lavoro, non prevista nell'autorizzazione alla trasferta, sarà retribuita come lavoro straordinario soltanto se eseguita per documentate attività di interesse aziendale (esempi: partecipazioni ad assemblee dei soci, a consigli di amministrazione, e simili), ovvero per seri e comprovati motivi che il responsabile dell'ufficio valuterà caso per caso.

A 5.3 – I rimborsi delle spese vengono effettuati con il sistema del rimborso a piè di lista. I limiti di spesa sono i seguenti:

TRENI: utilizzo della prima e seconda classe;
PASTI: tetto giornaliero di euro 60,00;
AEREI: per le distanze superiori a 300 KM – qualora la destinazione sia servita da più vettori – si dovrà preferire il vettore più economico tenendo conto della durata del viaggio;
AUTO A NOLEGGIO: il dipendente dovrà utilizzare i servizi delle società convenzionate con l'azienda, utilizzando autovetture del gruppo C per percorsi fino a 300 KM;
ALBERGHI: il dipendente ha un tetto massimo di spesa pari a euro 110,00 a notte, derogabile soltanto con la preventiva autorizzazione dell'azienda. Le prenotazioni verranno effettuate dalla segreteria presso le strutture convenzionate con l'azienda;
TAXI: l'uso del taxi è consentito per le partenze ed i rientri fuori l'orario di lavoro;
SPESE TELEFONICHE: per i dipendenti che non sono assegnatari di un telefono mobile aziendale, le spese telefoniche vengono riconosciute sulla base delle schede telefoniche presentate: l'azienda si riserva fin da ora di apportare modifiche in relazione all'uso privato e personale per coloro i quali sono assegnatari del telefono mobile aziendale, così come previsto dalla normativa fiscale in relazione ai "fringe benefits";

RIMBORSO CHILOMETRICO: viene calcolato sulla base di euro 0,45 a Kilometro, in relazione all'itinerario più razionale per il raggiungimento delle destinazioni, tenuto conto anche dei tempi di viaggio;

A 5.4 – Il caposervizio autorizza la nota spese e l'amministrazione aziendale, verificata la congruità delle spese richieste a rimborso, liquida la nota spese al dipendente.

B) PROVVEDIMENTI DISCIPLINARI

Per quanto riguarda i provvediamenti disciplinari, le ammonizioni scritte e verbali, le multe e le sospensioni, nonché i licenziamenti si fa riferimento integrale all'art. 225 del CCNL.

C) SICUREZZA

Metodologia seguita nella valutazione dei rischi
La metodologia seguita nell'analisi dei rischi ha tenuto conto del contenuto specifico del dlgs 626/94, della circolare del ministero del lavoro n. 102/95 in data 7/8/95 e dei documenti emessi dalla Comunità europea.
Da un punto di vista generale il decreto impone che la relazione sulla valutazione dei rischi debba contenere una *descrizione dei «criteri adottati per la valutazione stessa»* (art. 4, comma 2, a).
Questo orientamento di fondo è ripreso e confermato nel documento *Orientamenti riguardo alla valutazione dei rischi sul lavoro,* emesso da Comunità europea Dg v/e/2 unità medicina e igiene del lavoro (Cee), allo scopo di «fornire orientamenti riguardo alle modalità della valutazione dei rischi sul lavoro» attraverso una descrizione dei «passi da compiere in vista dell'identificazione dei mezzi più opportuni per eliminare i rischi, oppure per controllarli».
L'obiettivo della valutazione dei rischi consiste nel consentire al datore di lavoro di prendere i provvedimenti che sono effettivamente necessari per salvaguardare la sicurezza e la salute dei lavoratori.
Uno *strumento generale* di valutazione dei rischi professionali dovrà quindi rifarsi, almeno in prima istanza, a *criteri operativi semplificati* che consentano di soddisfare comunque ad alcuni requisiti, peraltro definiti in altrettante fasi dalle stesse linee guida europee:
1. assicurare la maggiore sistematicità possibile al fine di garantire l'identificazione di tutti i possibili rischi presenti; volendo specificare più in dettaglio, questo include due momenti concettualmente distinti:

individuazione e caratterizzazione delle fonti potenziali di pericolo (sostanze, macchinari, agenti nocivi ecc...).
Questa fase deve consentire di conoscere le evidenze oggettive di tipo tecnico e organizzativo che possono generare rischi per i lavoratori. Il rischio si genera nel caso in cui, evidentemente, siano presenti lavoratori esposti a ciascuna fonte individuata;

individuazione e caratterizzazione dei soggetti esposti: esame di ciascun gruppo di soggetti esposti alla fonte di pericolo e individuazione del tipo di esposizione in funzione di una molteplicità di parametri, che vanno rilevati *(fattori di prevenzione e protezione dei soggetti a rischio)*, quali:

- grado di formazione/informazione;
- tipo di organizzazione del lavoro ai fini della sicurezza;
- influenza di fattori ambientali, psicologici specifici;
- presenza e adeguatezza dei dispositivi di protezione individuale;
- presenza e adeguatezza di sistemi di protezione collettivi;
- presenza e adeguatezza di piani di emergenza, evacuazione, soccorso;
- sorveglianza sanitaria.

2. Procedere alla valutazione dei rischi in senso stretto, per ciascuno dei rischi individuati alla fase 1: ciò significa poter emettere un giudizio di gravità del rischio e quindi di conformità e adeguatezza della situazione in essere, rispetto alle esigenze di prevenzione e protezione dai rischi.
3. Consentire l'individuazione delle misure di prevenzione e protezione da attuare in conseguenza degli esiti della valutazione e stabilire il programma di attuazione delle stesse in base a un ordine di priorità.

L'impianto metodologico della valutazione è stato definito a partire dai dettami del decreto e dalle linee-guida emesse in proposito a livello Ue e a livello di organizzazioni pubbliche e private degli stati membri.
Si procede alla valutazione tramite una verifica riguardante i fattori di rischio seguenti:

Elenco dei fattori di rischio (tab.1)

RISCHI PER LA SICUREZZA DEI LAVORATORI
1. Aree di transito
2. Spazi di lavoro
3. Scale
4. Macchine
5. Attrezzi manuali
6. Manipolazione manuale di oggetti
7. Immagazzinamento di oggetti
8. Impianti elettrici
9. Apparecchi a pressione
10. Reti e apparecchi distribuzione gas
11. Apparecchi di sollevamento
12. Mezzi di trasporto
13. Rischi di incendio ed esplosione
14. Rischi per la presenza di esplosivi
15. Rischi chimici
RISCHI PER LA SALUTE DEI LAVORATORI
16. Esposizione ad agenti chimici
17. Esposizione ad agenti cancerogeni

18.	Esposizione ad agenti biologici
19.	Ventilazione industriale
20.	Climatizzazione locali di lavoro
21.	Esposizione a rumore
22.	Esposizione a vibrazioni
23.	Microclima termico
24.	Esposizione a radiazioni ionizzanti
25.	Esposizione a radiazioni non ionizzanti
26.	Illuminazione
27.	Carico di lavoro fisico
28.	Carico di lavoro mentale
29.	Lavoro ai video terminali
ASPETTI ORGANIZZATIVI E GESTIONALI	
30.	Organizzazione del lavoro
31.	Compiti, funzioni e responsabilità
32.	Analisi, pianificazione e controllo
33.	Formazione
34.	Informazione
35.	Partecipazione
36.	Norme e procedimenti di lavoro
37.	Manutenzione
38.	Dispositivi di protezione individuale
39.	Emergenza, pronto soccorso
40.	Sorveglianza sanitaria

Vi sono tre categorie di fattori di rischio:

I. rischi per *l'incolumità fisica dei lavoratori* (dal n. 1 al n. 15);
II. rischi per la *salute dei lavoratori* (dal n. 16 al n. 29);
III. il terzo gruppo (dal n. 30 al n. 40) comprende più propriamente una serie di fattori gestionali di prevenzione, in quanto in essi vengono esaminate le misure generali di *tutela e prevenzione presenti a livello aziendale*, aventi a che fare con gli aspetti organizzativi, formativi, procedurali.

Per «fattore di rischio» si deve quindi intendere ogni aspetto che può in qualche modo generare o influenzare il livello di rischio professionale individuabile all'interno delle attività aziendali, si tratti di fattori materiali (sostanze pericolose, macchinari ecc.) o di fattori organizzativi e procedurali (sorveglianza sanitaria, piani di emergenza, istruzioni, libretti di manutenzione ecc.).

Il fattore di rischio viene analizzato sotto i due principali aspetti che caratterizzano la fase dell'identificazione dei rischi:

le diverse tipologie e forme che le *fonti di pericolo* connesse a quel fattore di rischio possono assumere e, contestualmente, le diverse misure protettive e preventive che ciascuna di esse può o deve presentare;
le diverse misure di prevenzione e protezione che i *soggetti a rischio* possono o debbono avere, sia di tipo collettivo che individuale, legate per lo più ad aspetti *organizzativi e formativi.*
Nell'analisi del fattore di rischio i vari punti di verifica sono stati esplicitati tenendo presenti, in linea generale, tre classi di riferimenti:
le richieste specifiche della normativa in vigore;
gli standard internazionali di buona tecnica;
la rispondenza al «buon senso ingegneristico»
Questo significa che la verifica è stata effettuata mediante l'analisi accurata della normativa vigente e degli standard internazionali di buona pratica, integrando questo insieme di norme e standard, ove possibile, con indicazioni derivanti dal buon senso ingegneristico.
L'insieme delle risultanze della verifica, delle valutazioni e delle indicazioni delle azioni correttive e della loro priorità, costituisce il cuore del documento di valutazione dei rischi da custodire in azienda, richiesto dal dlgs 626/94, in quanto ne contiene tutti gli elementi essenziali (art. 4, comma 2):
la relazione sulla valutazione dei rischi;
l'individuazione delle misure di prevenzione e protezione da attuare e delle attrezzature di protezione (rintracciabili nei singoli punti di verifica);
il programma di attuazione delle misure (priorità, così come scaturiscono dalle valutazioni delle carenze riscontrate).

Rischi legati ad aspetti generali dell'organizzazione
Il lavoro è svolto secondo procedure chiare e note ai lavoratori, alla formulazione delle quali gli stessi sono stati chiamati a contribuire.
Compiti, funzioni e responsabilità sono chiaramente assegnati e distribuiti rispettando le competenze professionali.
È stato organizzato il servizio di prevenzione e protezione ai sensi del dlgs 626/94 e nominato il responsabile del servizio nella persona del Dott. Paolo de Sarno Prignano.
È stato definito un programma per il raggiungimento di obiettivi concreti in tema di prevenzione dei rischi.
L'azienda intende svolgere con frequenza almeno annuale la riunione periodica di prevenzione e protezione dai rischi.
Tutti i lavoratori ricevono un'informazione e una formazione sufficienti e adeguate, specificamente incentrate sui rischi relativi alla mansione ricoperta.
Esiste un piano di emergenza il cui contenuto è adeguato alle necessità dell'azienda, noto ai lavoratori.
Esiste un servizio di pronto soccorso.
Esiste una collaborazione attiva fra datore di lavoro (Responsabile del Servizio di prevenzione e protezione) e rappresentante dei lavoratori.

Coinvolgimento delle componenti aziendali
Nell'effettuazione della valutazione si è tenuto conto dei commenti e delle osservazioni dei lavoratori coinvolti.
Il piano sulla valutazione dei rischi deve essere preso in visione da tutti i lavoratori.

Processi per il miglioramento del livello di sicurezza
Videoterminali:
i videoterminali sono posti in modo tale da consentire lo svolgimento dell'attività lavorativa in maniera adeguata.

Oggetti:
si è provveduto ad una sistemazione razionale ed ordinata degli oggetti utilizzati in modo da diminuire il rischio di caduta o di un contatto accidentale con gli stessi.

Immagazzinamento di oggetti:
si è provveduto ad eliminare dal luogo di lavoro tutti quegli oggetti che non sono immediatamente utilizzati nelle lavorazioni riservando ad essi un apposito spazio.

Carico di lavoro fisico e mentale:
sono sempre previste delle pause anche quando il carico di lavoro supera i valori normali.

Organizzazione del lavoro:
quando è possibile è data l'opportunità di alternare le normali mansioni dell'attività lavorative, inoltre sono dati tutti quei suggerimenti per svolgere nella maniera migliore tali mansioni. Sono state inoltre precisate le attività che non devono essere svolte dai lavoratori (a causa, ad esempio, della specializzazione occorrente).

Formazione: ogni qualvolta se ne presenti la necessità viene fornita una formazione sufficiente in relazione alle mansioni svolte. I lavoratori sono informati sulle modalità di svolgimento delle attività.
I lavoratori sono informati riguardo alla corretta posizione da assumere nelle postazioni di lavoro.
I lavoratori sono informati riguardo la protezione della vista e degli occhi.

Partecipazione :
è stato richiesto ai lavoratori di fornire quei suggerimenti e quelle indicazioni necessarie per migliorare la sicurezza nelle mansioni a cui sono preposti.

Norme e procedimenti:
Le procedure di lavoro sono state adeguatamente divulgate a tutti gli interessati in modo da non creare incertezze e conseguenti rischi.

Emergenza e pronto soccorso: è stato predisposto un adeguato piano di emergenza comprendente un piano antincendio e un piano di evacuazione.

D) PRIVACY

Il D.L. 675/96 ed il D.P.R. 318/99
La legge che tutela i dati personali é la legge 675/96 “Tutela delle persone e di altri soggetti rispetto ai trattamenti di dati personali” del 31 dicembre 1996.
Il regolamento attuativo di tale legge è stato pubblicato sulla gazzetta ufficiale in data 28 luglio 1999: il D.P.R. 318/99, “Regolamento recante le norme per l’individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell’art.15, comma 2 della legge 675/96”.
Il regolamento attuativo determina le norme minime di sicurezza che devono essere garantite in una struttura informatica e i soggetti incaricati alla loro applicazione.
Le norme sono differenziate a seconda che la struttura informatica abbia o meno una certa topologia di rete, ovvero che gli archivi contenenti dati personali siano o meno accessibili da altri calcolatori e similmente, i soggetti incaricati hanno differenti responsabilità.

I soggetti incaricati
Le figure individuate dalla legislazione sono:
il *titolare*: la persona fisica o giuridica alla quale è da riferirsi la titolarità del trattamento ed i conseguenti oneri facoltà, ivi compreso il profilo della sicurezza;
il *responsabile*: come previsto dagli articoli 1 e 8 del D.L. 675/96, è la persona (fisica, giuridica, ente, associazione, . .) che, se designata, è stata preposta dal titolare al trattamento dei dati personali; tale persona, per esperienza, capacità e affidabilità fornisce idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
gli *amministratori di sistema*: essi sono i soggetti preposti al compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di dati e di consentirne l’utilizzazione;
i soggetti preposti alla custodia delle parole chiave, soggetti preposti alla custodia dei codici identificativi personali, soggetti preposti alla custodia di chiavi per strumenti di custodia di documenti: la funzione di tali soggetti è limitata all’ambito del controllo e della custodia delle parole chiave, dei codici identificativi o delle chiavi fisiche che fungono da codice di accesso a parti della struttura informatica.
Il responsabile è tenuto ad indentificare e a designare per iscritto sia gli amministratori di sistema che tutti gli altri soggetti sopra indicati. Costoro, analogamente, sono tenuti a rispettare i regolamenti e le direttive loro assegnate, dal presente documento, per l’applicazione delle misure di sicurezza.

Le definizioni dei dati
Ai sensi dell’art. 1, comma 2 lett. C della legge 675/96, per “dato personale” si intende una qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
L’interpretazione del testo di legge porta a suddividere i dati così come definiti in due diverse categorie:

dati cosiddetti neutri (la definizione è data *ad escludendum* rispetto alle definizioni successive); si tratta di tutti quei dati che, pur personali, non presentano alcuna particolarità ovvero informano circa una situazione non ritenuta degna di particolare tutela dell’ordinamento (ad esempio indirizzi, numeri telefonici,……).

dati particolari la cui definizione è tratta dal capo IV della legge 675/96 e comprende le seguenti categorie di dati:
dati sensibili (così come definiti dell'art. 22 comma 1 della legge);
sono i dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni ed organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale,
dati relativi ai provvedimenti di cui all'art. 686 del codice di procedura penale; sono definiti dall'art. 24 della legge 675/96 e riguardano appunto i provvedimenti suddetti, ovvero le iscrizioni nel casellario giudiziale relative ad un determinato soggetto.

Misure minime di sicurezza
Le misure minime di sicurezza fissate dal D.P.R. 318/99 sono differenti, a seconda del fatto che:
1. il trattamento dei dati personali sia effettuato per fini esclusivamente personali
2. il trattamento dei dati personali non sia effettuato per fini esclusivamente personali: in tal caso è necessario distinguere tra
(a) trattamento con strumenti diversi da quelli elettronici o comunque automatizzati oppure
(b) trattamento con strumenti elettronici o comunque automatizzati:
in tal caso è necessario distinguere tra
i. trattamento effettuato mediante elaboratori non accessibili da altri elaboratori o terminali,
ii. trattamento effettuato mediante elaboratori accessibili in rete, siano esse reti non disponibili al pubblico che reti di telecomunicazione disponibili al pubblico.

Si hanno pertanto quattro casi diversi:
Trattamento dei dati personali effettuato per fini esclusivamente personali
Indipendentemente dal fatto che gli elaboratori siano o meno accessibili da altri elaboratori o terminali, solo nel caso in cui i dati siano organizzati in una banca dati è necessario proteggere l'accesso ai dati o al sistema mediante una parola chiave.
La parola chiave deve essere diversa per i differenti utilizzatori in presenza di dati organizzati per banche dati. La banca dati (come descritto nell'articolo 2 del D.L. 675/96) è un complesso di dati, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento.

Trattamento dei dati personali per fini non esclusivamente personali con strumenti diversi da quelli elettronici o comunque automatizzati
Si applicano le disposizioni indicate nell'articolo 9 del D.P.R. 318/99:
nel nominare per iscritto gli incaricati del trattamento è necessario specificare che costoro abbiano accesso solamente ai dati personali la cui conoscenza sia necessaria allo svolgimento dei compiti loro assegnati,
gli atti ed 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.
Inoltre, nel caso si tratti di dati di cui agli articoli 22 e 24 della legge 675/96, si deve ulteriormente garantire che:

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

Trattamento dei dati personali per fini non esclusivamente personali effettuato mediante elaboratori non accessibili da altri elaboratori o terminali
In tale caso si applicano le misure indicate nell'articolo 2 del D.P.R. 318/99.
Essenzialmente ciò si riduce ad avere un sistema di parole chiave predisposto al controllo degli accessi ai dati:
devono essere individuati per iscritto uno o più soggetti preposti alla custodia delle parole chiave e alla loro eventuale sostituzione,
le parole chiave devono essere fornite ad ogni singolo incaricato del trattamento, deve essere previsto, se possibile, un meccanismo autonomo che consenta ai medesimi incaricati la sostituzione delle proprie parole chiave, previa comunicazione agli addetti responsabili.

Trattamento dei dati personali per fini non esclusivamente personali effettuato mediante elaboratori accessibili attraverso reti pubbliche o meno
In questo caso è necessario preventivamente accertarsi che siano state applicate le norme di sicurezza del punto precedente (l'esistenza di parole chiave, di soggetti preposti alla loro custodia) e le seguenti disposizioni aggiuntive:
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 può, neppure in tempi diversi, essere assegnato a persone diverse;
i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'articolo 615 quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.

Accesso ai dati sensibili
Nel caso in cui il trattamento riguardasse anche i dati di cui agli articoli 22 e 24 della legge 675/96, il responsabile del trattamento deve rilasciare agli incaricati del trattamento delle autorizzazioni (per persona singola o per gruppo di lavoro), suscettibili dei seguenti vincoli:
L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.
Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.
L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.
La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso.

Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro. Tale norma implica che tutti i programmi che trattano dati di cui agli articoli 22 e 24 della legge 675/96 (ossia ciò che nella legge è nomato applicazione) debbano prevedere un meccanismo di autenticazione che impedisca a più utenti che condividono lo stesso codice identificativo personale di accedervi contemporaneamente. Infine, anche i supporti di memorizzazione utilizzati durante il trattamento dei dati di cui agli articoli 22 e 24 della legge 675/96 possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

Documento programmatico sulla sicurezza

Nel caso il cui il trattamento dei dati personali riguardasse i dati di cui agli articoli 22 e 24 della legge 675/96, la legge (articolo 6 del D.P.R. 318/99) prevede la predisposizione e l'aggiornamento con cadenza annuale di un documento, definito "Documento programmatico sulla sicurezza" dei dati.

Per la redazione del documento è necessario compiere un'analisi dei rischi al fine di distribuire i compiti e le responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi. Secondo il regolamento, il documento programmatico sulla sicurezza deve definire:

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;

i criteri e le procedure per assicurare l'integrità dei dati;

i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;

l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

Responsabilità civile per il trattamento dei dati

Occorre inoltre ribadire che le misure minime indicate nel D.P.R. 318/99 devono considerarsi necessarie ma non sufficienti. Il rispetto di tali misure non rappresenta infatti una esimente nel caso in cui vengano arrecati danni a terzi per effetto del trattamento di dati personali. Il preciso riferimento all'art. 2050 del codice civile (Responsabilità per l'esercizio di attività pericolose) fa sì che, in caso di procurato danno, resti a carico del titolare del trattamento la dimostrazione di avere adottato tutte le misure cautelative capaci di prevenire il danno stesso.

Alla luce ti tali implicazioni legali è chiaro come sia necessario adoperarsi al meglio, onde essere in grado di potere dimostrare che, nell'eventualità di vertenze legate alla responsabilità civili dei responsabili del trattamento dei dati personali, fosse stata presa ogni possibile misura per garantire la massima sicurezza possibile della struttura informatica.

L'approccio seguito nel seguito di questo documento, soprattutto per le parti di pertinenza delle figure responsabili, consta nell'individuare nella pratica della sicurezza (informatica, ma non solo) le migliori procedure in uso e di attenersi, nei limiti del possibile, a tali direttive.

Ruolo e compiti del responsabile del trattamento dei dati personali

Il presente capitolo indica quali sono i ruoli ed i compiti dei responsabili della sicurezza e del trattamento dei dati personali. Lo scopo dei due ruoli, che possono coincidere, e che sovente coincidono per ragioni di praticità, è rispettivamente:

per i *responsabili della sicurezza* nell'individuare e rendere operative le procedure necessarie a garantire il rispetto della politica aziendale, sia al momento dell'applicazione del presente documento che nel tempo;
per i *responsabili del trattamento dei dati personali* nell'essere la persona preposta dal titolare al trattamento dei dati personali *"che per esperienza, capacità ed affidabilità fornisce garanzia del rispetto delle vigenti disposizioni in materia"*, anche con riferimento al profilo della sicurezza (Art.8, legge 675/96).

Compiti del responsabile del trattamento
Il responsabile del trattamento dei dati personali ha i seguenti compiti:
1. rispettare e fare rispettare le misure prescritte dalla legge;
2. sottoscrivere le notifiche e le variazioni da comunicarsi al Garante dei trattamenti dei dati personali, attività questa da svolgersi assieme al titolare dell'esercizio.
3. controllare l'operato degli incaricati del trattamento dei dati personali.
4. controllare che il trattamento dei dati personali avvenga nell'ambito della legittimità del rapporto di lavoro, verificando pertanto che essi siano acceduti, utilizzati, modificati e distrutti in modo corretto.
Il responsabile si avvale di incaricati del trattamento dei dati personali, ossia di persone che per scopi di lavoro necessitano di trattare i dati personali posseduti dall'azienda.

Rapporti con il titolare
Il responsabile del trattamento dei dati personali deve riportare periodicamente al titolare una relazione relativa agli adempimenti di legge operati. Deve inoltre comunicare al titolare:
le richieste degli interessati di accesso, blocco, cancellazione e opposizione al trattamento dei dati personali:
informare il titolare di ogni questione rilevante ai fini legali, derivante dall'operato di soggetti interessati o dal Garante stesso;
il trattamento o il trasferimento di dati personali all'estero (di ciò deve essere data comunicazione al Garante, Art. 28, legge 675/96).

Rapporti con i collaboratori e gli incaricati
Il responsabile del trattamento dei dati personali ha il compito di sorvegliare che gli incaricati del trattamento dei dati personali operino entro le norme stabilite dalla legge. Si osservi che non si considera comunicazione la conoscenza dei dati personali da parte di persone incaricate per iscritto
di compiere le operazioni del trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta autorità (Art. 19, legge 675/96).
Il responsabile deve pertanto controllare che siano rispettate le disposizioni impartite (Art. 8, legge 675/96), che non vengano trattati dati personali senza che i rispettivi interessati ne abbiano dato il consenso e che, cessato il rapporto di collaborazione, tutti i dati personali detenuti, in forma elettronica e cartacea, siano restituiti o distrutti.

Rapporti con gli interessati
Il responsabile del trattamento dei dati personali deve infine disporre dell'applicazione della legge 675/96, in particolare degli articoli 10 e11, per quanto riguarda i rapporti con gli interessati del trattamento dei dati personali. I dati personali oggetto di trattamento devono essere:
1. trattati in modo lecito e secondo correttezza;

2. raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
3. esatti ed aggiornati;
4. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati,
5. 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 (Art. 9, legge 675/96).

È compito del responsabile del trattamento dei dati personali fare sì che ogni incaricato del trattamento, qualora si presenti l'occasione di raccogliere o registrare nuovi dati, accerti altresì il consenso dei medesimi interessati, li informi dei loro diritti ai sensi dell'articolo 13 della legge
675/96, e in caso di consenso faccia firmare l'apposita lettera informativa o controlli la presenza della stessa.

Il responsabile deve successivamente operare affinché le informative siano archiviate e conservate per futura evidenza della corretta raccolta e del corretto utilizzo dei dati.

Il responsabile deve infine pianificare le procedure necessarie ad evadere celermente le richieste degli interessati nel caso questi esercitassero i diritti indicati nell'articolo 13 della legge 675/96, ovvero:
1. il diritto a conoscere dell'esistenza di dati che lo riguardino, la loro natura e la loro finalità;
2. il diritto alla cancellazione, alla rettifica, all'aggiornamento, alla trasformazione o al blocco dei dati che lo riguardano;
3. il diritto di opporsi al trattamento dei dati, ancorché pertinenti allo scopo della raccolta;
4. il diritto di opporsi al trattamento dei dati previsto a fini di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva e di essere informato dal titolare, non oltre il momento in cui i dati sono comunicati o diffusi, della possibilità di esercitare gratuitamente il diritto (Art.13, legge 675/96).

Si consideri infatti che, trascorsi cinque giorni dalla richiesta, l'interessato può proporre ricorso al Garante per la tutela dei dati personali, ovvero adire l'autorità giudiziaria competente.

E) GESTIONE COMPUTERS AZIENDALI, PROGRAMMI,INTERNET

E 1 - GESTIONE COMPUTERS AZIENDALI, PROGRAMMI , INTERNET

Si rammenta a tutto il personale dipendente che l'uso dei personal computers aziendali e' severamente vietato per usi personali, cosi come altrettanto e' vietato l'uso improprio e personale di programmi contenuti nei personal computers aziendali.
Si rammenta inoltre di prestare la massima attenzione nell'uso dei collegamenti internet e motori di ricerca di ogni tipo.
SI RICORDA INFINE, CHE E' SEVERAMENTE VIETATO INTRODURRE NEL COMPUTER DI PROPRIA ASSEGNAZIONE PROGRAMMI PER USO PERSONALE PRIVI DI LICENZA E NON AUTORIZZATI DALL'AZIENDA, NONCHE' CHE E' ALTRETTAMENTO SEVERAMENTE VIETATO IMPORTARE DALLA RETE INTERNET, DAI MOTORI DI RICERCA E QUANT'ALTRO SIMILE ALL'INTERNO DEL PERSONAL COMPUTER ASSEGNATO "PROGRAMMI, DI QUALSIASI TIPO "NON LICENZIATI E NON AUTORIZZATI ALL'USO PUBBLICO".

L'AZIENDA RISERVA AGLI EVENTUALI TRASGRESSORI DI QUANTO QUI RIPORTATO L'APPLICAZIONE DELLA DISCIPLINA PREVISTA IN TUTTI I CAPITOLI DELLA LETTERA "B" DEL PRESENTE REGOLAMENTO.

L'AZIENDA SI RISERVA INFINE, IN CASO DI CONTROLLO E DI EVENTUALE SANZIONE, OLTRE ALL'APPLICAZIONE DELLA DISCIPLINA REGOLAMENTARE, ANCHE TUTTI I PROCEDIMENTI LEGALI PER IL RIADDEBITO A CARICO DEL CONTRAVVENTORE DELLA SANZIONE RICEVUTA.