AMIA VERONA SPA
AZIENDA MULTISERVIZI
DI IGIENE AMBIENTALE

AMIA Verona S.p.a.
Prot. N. 10806/P20
del 18.09.2010

ACCORDO SINDACALE N. 6/2010

OGGETTO: Policy Aziendale.

Verona, 8 settembre 2010

tra

l'AMIA Verona S.p.A. rappresentata dal Direttore Generale Ing. Giampietro Cigolini

e

le R.S.A. rappresentate dai Signori:

per la FP CGIL - Sig. Loi Antonio

per la FIT CISL - Sig.ra Martelli Gabriella

per la UILT - Sig. Simone Livio

per la CISAL Enti Locali e Servizi - Sig. Corrizzato Alberto

per la UGL - Sig. Fermo Angelo

premesso che

- La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai personal computer, espone AMIA Verona Spa ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine della Società stessa;

- L'utilizzo delle risorse informatiche e telematiche della Società deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, ai sensi del punto 19 del D.Lgs. 196/03 "Codice in materia di protezione dei dati personali e del provvedimento del Garante per la Protezione dei dati Personali del 1° marzo 2007, AMIA Verona Spa ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati

37135 Verona
Via B. Avesani, 31
Tel. 045 8063311
Fax 045 8069027

www.amiavr.it
amia.verona@amiavr.it

Casella Postale
1053 vr succ. 10

Registro Imprese
n. 02737960233

Cap. Soc. int. vers.
€ 12.804.138,00

C. F. e P. IVA
02737960233

Società soggetta ad attività di direzione e coordinamento del Comune di Verona Socio Unico

AMIA VERONA SPA
AZIENDA MULTISERVIZI
DI IGIENE AMBIENTALE

si conviene

1. Di prendere atto delle linee guida comportamentali per il trattamento sicuro dei dati e per il corretto utilizzo di strumenti informatici, apparecchi telefonici, posta elettronica ed internet in ambito lavorativo definite nel documento "Policy Aziendale", approvato dal Consiglio di Amministrazione nella seduta del 29 giugno 2010 con deliberazione n° 19.

Direttore Generale Ing. Giampietro Cigolini

FP CGIL –

FIT CISL –

UILT –

CISAL Enti Locali e Servizi –

UGL –

POLICY AZIENDALE

Linee Guida Per il Corretto Utilizzo di Strumenti informatici, Apparecchi telefonici, Posta elettronica ed Internet in ambito lavorativo

(ai sensi del punto 19 del D.lgs. 196/03 "Codice in materia di protezione dei dati personali"

e del provvedimento del Garante per la Protezione dei dati Personali del 1 marzo 2007)

INDICE

VERSIONE DEL DOCUMENTO **3**

POLICY AZIENDALE **4**

1 - PREMESSA **4**

2 - PRINCIPI GENERALI **5**

2.1 - TUTELA DEL LAVORATORE 5
2.2 - DIRITTI ALLA PROTEZIONE DEI DATI PERSONALI 5
2.3 - PRINCIPIO DI TRASPARENZA 5

3 - DEFINIZIONI **6**

3.1 - DISPOSITIVI INFORMATICI 6
3.2 - RETE INTERNET 6
3.3 - POSTA ELETTRONICA 6
3.4 - SOFTWARE AZIENDALE 6
3.5 - IMPIANTI TELEFONICI AZIENDALI 6

4 - REGOLE DI UTILIZZO **7**

4.1 - DISPOSITIVI INFORMATICI 7
4.2 - RETE INTERNET 8
4.3 - POSTA ELETTRONICA 8
4.4 - SOFTWARE AZIENDALE 9
4.5 - IMPIANTI TELEFONICI AZIENDALI 9
4.6 - PROTEZIONE DATI TRAMITE SISTEMI DI CIFRATURA O PASSWORD 10
4.7 - ISTRUZIONI IMPARTITE DAL TITOLARE 10

5 - CONTROLLI E CORRETTEZZA NEL TRATTAMENTO **11**

5.1 - RETE INTERNET – FORME DI CONTROLLO 11
5.2 - RETE INTERNET - GARANZIE PER IL LAVORATORE 12
5.3 - POSTA ELETTRONICA - FORME DI CONTROLLO 12
5.4 - POSTA ELETTRONICA - GARANZIE PER IL LAVORATORE 13
5.5 - IMPIANTI TELEFONICI AZIENDALI 14
5.6 - Forme di controllo generali *14*
5.7 - Garanzie per il lavoratore *14*

6 - SOGGETTI COINVOLTI **15**

6.1 - RESPONSABILI DEL TRATTAMENTO 15
6.2 - AMMINISTRATORI DI SISTEMA 15
6.3 - FIDUCIARI 15

7 - SANZIONI **16**

8 - DISPOSIZIONI GENERALI **17**

VERSIONE DEL DOCUMENTO

Novità introdotte rispetto alla precedente emissione

REVISIONE					
N°	Data	Descrizione	Emesso	Verificato	Approvato
0	28/05/2010				

POLICY AZIENDALE

1 - PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai personal computer, espone AMIA SpA ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine della Società stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della Società deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, AMIA SpA ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

L'individuazione di regole precise e chiare per l'utilizzo delle risorse interne dell'azienda, da parte dei dipendenti e dei collaboratori, è un passaggio obbligato nel percorso che porta all'ottimizzazione del funzionamento dell'impresa. Solo attraverso la creazione di un codice etico, rivolto verso l'interno del complesso aziendale, atto a regolare i rapporti con il personale interno e contenente garanzie reciproche tra le parti è possibile gestire le problematiche legali e gestionali che derivano dall'esercizio dell'attività.
Sono proprio questi gli elementi che hanno ispirato la direzione nella stesura delle norme di comportamento conformi alle leggi ed ai principi di giustizia e garanzia dei diritti del singolo. E' la comprensione delle ragioni che animano le regole di comportamento che porta al loro rispetto spontaneo.

Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Decreto Legislativo 196/03 in materia di trattamento dei dati personali e misure minime di sicurezza e sono coordinate con quanto previsto dal Provvedimento Del garante della Privacy del primo marzo 2007.

2 - PRINCIPI GENERALI

2.1 - Tutela del Lavoratore

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali.

2.2 - Diritti alla protezione dei dati personali

Nell'impartire le seguenti prescrizioni AMIA SpA tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (*artt. 1 e 2, D.Lgs. 196/03 – Codice in materia di protezione dei dati personali, di seguito Codice*). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica. I trattamenti rispettano le garanzie in materia di protezione dei dati e si svolgono nell'osservanza dei principi di *necessità, correttezza, per finalità determinate, esplicite* e *legittime* osservando il principio di *pertinenza* e *non eccedenza e nella misura meno invasiva possibile.*

2.3 - Principio di trasparenza

In base al richiamato principio di correttezza, la AMIA SpA ispira il presente regolamento ad un canone di trasparenza, come prevede anche la disciplina di settore (*art. 4, secondo comma, Statuto dei lavoratori; allegato VII, d.lg. n. 81/08 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali").*

3 - DEFINIZIONI

3.1 - Dispositivi informatici

Si intendono come dispositivi informatici gli strumenti messi a disposizione del personale per svolgere attività lavorativa (Personal Computer fissi e portatili, Palmari, Hard Disk o lettori di vario genere, stampanti, schede UMTS).

3.2 - Rete internet

Per rete Internet si intende la rete mondiale di comunicazioni basata sul protocollo TCP/IP e più specificamente il World Wide Web e l'attività di navigazione all'interno dello stesso.

3.3 - Posta elettronica

Per servizio di posta elettronica interno si intende il sistema informatico su cui operano gli indirizzi di posta elettronica (e-mail) aziendali e da cui si possono inviare e ricevere messaggi di posta elettronica sia interni sia da e verso Internet.

3.4 - Software aziendale

Qualunque applicativo software utilizzato all'interno della struttura aziendale, accompagnato da regolare licenza d'uso, per svolgere attività lavorativa.

3.5 - Impianti telefonici aziendali

Per "impianti telefonici aziendali" si intendono tutte le infrastrutture tecniche e le apparecchiature, sia fisse sia mobili, atte alla comunicazione vocale ed in uso all'interno dell'azienda.

4 - REGOLE DI UTILIZZO

4.1 - Dispositivi informatici

I dispositivi informatici (Personal Computer fissi e portatili, Palmari, Hard Disk o lettori di vario genere, stampanti, schede UMTS) sono affidati al personale a seguito di esplicita e preventiva richiesta del responsabile funzionale, in collaborazione con l'Ufficio del Personale/Responsabile del Trattamento in caso di assunzioni o cambi mansione.

Sarà compito del responsabile funzionale, di concerto con il *Responsabile dei Sistemi Informativi* e l'Amministratore, valutare lo stato di obsolescenza del materiale affidato e prevedere dei piani di sostituzione dello stesso.

Tali apparati devono essere considerati come strumenti di lavoro e pertanto:

- vanno custoditi in modo appropriato (per i pc portatili si deve evitare l'abbandono, anche provvisorio, in luoghi quali uffici aperti, sale riunioni, bauli dell'automezzo in aree di parcheggio);
- **possono essere utilizzati esclusivamente per fini professionali e non anche per scopi personali;**
- devono essere prontamente segnalati alla Società di appartenenza il furto, il danneggiamento o lo smarrimento;
- nel caso di utilizzo di pc portatili all'esterno dell'azienda, conservare sul disco solo i files strettamente necessari;

In caso di furto o smarrimento, conseguenze del non rispetto delle regole di conservazione degli strumenti assegnati, potranno essere attivati dall'azienda meccanismi di rimborso del danno subito (bene e attività correlate).

Non è consentito in nessun caso, salvo espressa autorizzazione scritta da parte del *Responsabile dei Sistemi Informativi,* effettuare le seguenti operazioni:

- modificare le configurazioni impostate del proprio Pc (es.: installazione di masterizzatori, schede wireless, memoria RAM, schede audio/video, ecc.);
- installare sul PC propri mezzi di comunicazione (es.: modem, modem wireless, internet key ...);
- scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la prestazione lavorativa;
- eliminare i supporti magnetici non più utilizzabili (floppy disk, chiavi USB, cd/dvd rom, ecc.) in modo sicuro (distruzione fisica) o provvedere alla loro formattazione;
- attivare la password all'accensione (bios);
- far accendere i pc (boot) con dispositivi esterni (cd live, key usb, dischi usb);
- utilizzo di chiavi/hard disk usb non di uso aziendale;

E' responsabilità dei singoli incaricati (utilizzatori PC) applicare le seguenti procedure:

- non lasciare incustodito il Pc e bloccarlo in caso di assenza (utilizzando il comando Ctrl_Alt_Canc + invio);
- non utilizzare eventuali supporti di backup esterni se non per espresso assenso del Responsabile del Trattamento;
- utilizzare le unità di rete condivise per dislocare solamente files connessi all'attività lavorativa; la Società si riserva la facoltà di procedere, senza obbligo di preavviso, alla rimozione di ogni files o applicazione ritenuta pericolosa per la sicurezza del sistema o comunque di files acquisiti in violazione al presente Regolamento;
- in caso di intercettazione/sospetto di virus/malware/malfunzionamenti segnalare immediatamente il problema al *Responsabile dei Sistemi Informativi* o ai tecnici preposti, interrompendo qualunque elaborazione in corso;
- garantire il funzionamento delle procedure automatiche per l'aggiornamento di sistemi operativi e vari software (in caso di nuovi rilasci da parte dei produttori sarà cura del responsabile dei sistemi informativi attraverso i tecnici preposti provvedere ad installazioni/aggiornamenti).

4.2 - Rete internet

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale destinato esclusivamente allo svolgimento dell'attività lavorativa. La navigazione al fine di ricerca di informazioni deve limitare al minimo l'ingombro della banda di connessione; questo significa che le dimensioni dei file scaricati dovranno essere le più contenute possibili.

Sono vietate **in modo tassativo** le seguenti attività:

- navigazione in Internet in orario lavorativo per motivi diversi da quelli strettamente legati all'attività;
- utilizzo di modem privati per il collegamento alla rete / dispositivi esterni (internet key quando connessi alla rete aziendale ;
- download/upload di software non autorizzato o comunque non legato all'attività lavorativa;
- download/upload/ascolto/visione di file musicali, film e immagini non strettamente legati all'attività lavorativa;
- archiviazione sulla rete aziendale di qualunque file non connesso all'attività lavorativa;
- partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche anche utilizzando pseudonimi (o nicknames).
- Ascolto di radio via internet o visione di TV via internet

4.3 - Posta elettronica

L'indirizzo di posta elettronica è un bene aziendale e pertanto il suo utilizzo dovrà essere limitato a scopi esclusivamente di carattere professionale.

L'eventuale invio o ricevimento di e-mail di carattere personale dovrà avvenire solo mediante i servizi di web mail messi a disposizione dei vari provider internet. E' fatto assoluto divieto di scaricare i contenuti di tali e-mail.

Nel caso in cui il lavoratore riceva sulla propria casella di posta aziendale delle e-mail con allegati di cui non conosce con certezza la provenienza o con allegati sospetti (file con estensione tipo .exe .scr .pif .bat .cmd .txt vbs, js ...), **è tenuto a cancellarli senza aprirli** e ad avvisare il responsabile dei sistemi informativi.

Per quanto riguarda le comunicazioni interne tra dipendenti è necessario limitare al massimo l'estensione dei files inviati, soprattutto se non attinenti all'attività lavorativa, al fine di evitare un indebito sovraccarico delle linee.

Sono vietate in modo tassativo le seguenti attività:

- trasmissione di e-mail contenenti software non autorizzato o comunque non legato all'attività lavorativa;
- inoltro di messaggi il cui contenuto sia ingiurioso, diffamatorio o denigratorio, oppure offensivo, vessatorio, volgare, osceno o minatorio;
- trasmissione di e-mail contenenti file musicali, film e immagini non strettamente connesse all'attività lavorativa;
- iscrizione non autorizzata dal proprio responsabile a mailing list esterne;
- partecipazione a catene di e-mail di qualsiasi natura.

E' fatto obbligo agli incaricati di attivare le "regole fuori sede" eventualmente indicando l'indirizzo e-mail al quale rivolgersi per l'invio della comunicazione.

4.4 - Software aziendale

Qualunque applicativo software venga utilizzato all'interno della struttura aziendale deve essere accompagnato da regolare licenza d'uso. E' pertanto fatto tassativo divieto a chiunque utilizzi computer aziendali di scaricare dalla rete Internet qualsiasi software non autorizzato o installare sulle macchine stesse software di cui l'azienda sia priva di licenza d'uso provenienti dall'esterno. Qualunque nuova installazione dovrà essere espressamente autorizzata, per iscritto.

La violazione di questo principio comporta l'applicazione di sanzioni penali secondo quanto disposto dalla legge 633 del 1941 sul Diritto d'Autore.

Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della Legge n. 128 del 21.05.2004.

4.5 - Impianti telefonici aziendali

Gli impianti telefonici aziendali rientrano nella categoria dei "beni aziendali" e per questo il loro uso deve essere improntato alla tutela del patrimonio aziendale. Chi è autorizzato all'utilizzo degli stessi lo dovrà fare nel rispetto del principio indicato.

Chiunque usi gli impianti telefonici fissi per scopi estranei all'attività professionale a cui è addetto lo dovrà fare limitando il minimo i costi derivanti dalla telefonata. Da questo discende che l'uso degli impianti in questione per scopi privati è consentito in caso di necessità, ma limitato secondo le regole della correttezza e del buon senso. Per quanto concerne l'utilizzo dei telefoni mobili per scopi estranei all'attività professionale, dovrà avvenire premettendo al numero di interesse personale il numero 9.

4.6 - Protezione dati tramite sistemi di cifratura o password

E' fatto divieto, salvo deroghe, di cifratura o protezione con password di file o hard disk. In caso di autorizzazione da parte di un superiore di utilizzare password di protezione è fatto obbligo il deposito in busta chiusa sigillata e firrnata sui lembi di chiusura presso il responsabile del trattamento dei dati, il quale provvederà alla conservazione in cassaforte di tali buste, al fine di permettere all'azienda il pieno possesso dei propri dati. La password di amministrazione del dominio dovrà essere messa in busta chiusa sigillata per permettere all'azienda il pieno controllo sul suo sistema informativo.

4.7 - Istruzioni impartite dal titolare

E' obbligatorio attenersi alle ulteriori disposizioni impartite dal Titolare, ai sensi dell'art. 30 c.1 D.Lgs. 196/03.

5 - CONTROLLI E CORRETTEZZA NEL TRATTAMENTO

La AMIA SpA, utilizzando sistemi informativi per esigenze produttive o organizzative o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori (*art. 4, comma 2*), di sistemi che potrebbero consentire indirettamente un controllo a distanza e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Il trattamento di dati che ne consegue è considerato lecito.

La AMIA SpA rispetta le procedure di informazione e di consultazione di lavoratori in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

5.1 - Rete internet – Forme di controllo

La AMIA SpA, riduce il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), adottando opportune misure che possono, così, prevenire controlli successivi sul lavoratore.

In particolare, la AMIA SpA adotta le seguenti misure:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa; il software attualmente utilizzato da AMIA (interfaccia web ad oggi denominato FortiNet) blocca alla fonte tramite chiavi che vengono predisposte dal Responsabile dei Sistemi informativi la navigazione in tipologie di siti non ritenute "aziendali".
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni quali l'*upload* o l'accesso a determinati siti (inseriti in una *black list*) e/o il *download* di *file* .
- trattamento di dati di navigazione in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni;
- conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza;
- indicazione dei soggetti autorizzati all'accesso delle informazioni di cui al punto precedente;
- l'eventuale prolungamento dei tempi di conservazione sarà valutato e potrà avere luogo solo in relazione a:
    - esigenze tecniche o di sicurezza del tutto particolari;

  - indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
  - obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o di forze di polizia;
- controlli saltuari o occasionali per ragioni specifiche e non generiche, quali le verifiche sulla funzionalità e sicurezza del sistema. Tali verifiche verranno effettuate esclusivamente dal Responsabile del Trattamento per la Sicurezza dei Sistemi informatici, dagli incaricati alla manutenzione dei sistemi appositamente identificati e autorizzati. Tali ragioni possono essere:
  - Blocco del pc
  - Infezione da virus non rilevato dal sistema di sicurezza
  - Guasto di elementi hardware che rendono impossibile la prosecuzione dell'attività lavorativa
  - Instabilità o blocco di sistemi software
  - Altre cause
- la graduazione dei controlli: i controlli iniziali, riferibili a navigazioni non aziendali e comunque non autorizzate, saranno riferiti alla totalità e generalità degli utenti. In caso di estrema ratio, qualora si rilevino ulteriori abusi che possano precludere la sicurezza dei sistemi informativi, possano essere lesivi del patrimonio aziendale e possano identificare anche reati di natura penale, l'attività di controllo verrà effettuata con modalità di identificazione personale.

5.2 - Rete Internet - Garanzie per il lavoratore

Vista le delicatezza ed il carattere personale dei dati contenuti sui log, verranno adottate tutte le cautele necessarie per evitare di pregiudicare il diritto alla riservatezza del lavoratore, conformemente a quanto prescritto dal Codice.

AMIA SpA non utilizza sistemi hardware e software preordinati al controllo a distanza attraverso i quali sia possibile:

- effettuare controlli prolungati, costanti o indiscriminati;
- utilizzare strumenti di lettura e di registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
- effettuare analisi occulta di computer portatili affidati in uso.

5.3 - Posta elettronica - Forme di controllo

Con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica (@azienda.it/com), il lavoratore, in qualità di destinatario o mittente, utilizza la posta elettronica operando quale espressione dell'organizzazione datoriale.

Tale regolamento è quindi volto anche a sottolineare il carattere non personale ma aziendale della posta elettronica. Ciò garantisce la possibilità di AMIA SpA di verificare il contenuto dei messaggi in entrata e in uscita in base ai criteri di seguito elencati.

AMIA SpA adotta le seguenti soluzioni che contemperano le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza:

- L'indirizzo di posta elettronica fornito agli incaricati dall'azienda dovrà essere utilizzato solo ed esclusivamente per fini aziendali.
- Vengono messe a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze programmate (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura e relative istruzioni sull'utilizzo; l'utente dovrà servirsi delle "regole fuori sede" disponibili nel client di posta elettronica (menu "strumenti/regole fuori sede").
- L'apertura di messaggi di posta, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, viene gestita da soggetti fiduciari a verificare il contenuto dei propri messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa; AMIA SpA ha identificato come fiduciari per tutta l'organizzazione i Responsabili delle singole aree aziendali, salvo diverse disposizioni del lavoratore interessato;
- In caso di eventuali assenze non programmate (ad es., per malattia o infortunio) qualora il lavoratore non possa attivare la procedura di risposta automatica, tale funzione verrà attivata dai fiduciari di cui al punto precedente;
- I messaggi di posta elettronica dovranno contenere un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, con la precisazione che le risposte potranno essere visualizzate e conosciute da altri soggetti all'interno dell'azienda.

5.4 - Posta Elettronica - Garanzie per il lavoratore

In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato potrà delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Ciò non costituisce violazione del principio di segretezza della posta personale.

L'Azienda individua comunque come fiduciari in assenza di diversa disposizione del lavoratore, i Responsabili delle singole funzioni di cui al punto 6.3.

L'utilizzo di posta personale dovrà essere gestito dagli utenti tramite i servizi di Web Mail messi a disposizione di provider e gestori internet e tale utilizzo dovrà essere limitato negli orari di navigazione internet consentiti dal Titolare del Trattamento.

5.5 - Impianti telefonici aziendali

Nessun tipo di controllo personale verrà effettuato sulla natura delle telefonate effettuate. Il contenuto di esse è obbligatoriamente segreto ed ogni controllo in merito verrà effettuato utilizzando esclusivamente i tabulati forniti dai gestori di telefonia in armonia con le norme previste dall'attuale legislazione sulla Privacy.
Graduazione dei controlli: i controlli iniziali, riferibili a tempi di utilizzo eccessivi della rete telefonica aziendale, saranno riferiti alla totalità degli utenti. Il perdurare di tale anomala attività non consentita, autorizzerà l'azienda a scendere ulteriormente nel particolare effettuando controlli al livello di gruppi omogenei. In caso di estrema ratio, qualora si rilevino ulteriori abusi che possano essere lesivi del patrimonio aziendale, l'attività di controllo verrà effettuata con modalità di identificazione personale.

5.6 - Forme di controllo generali

Verranno effettuate rilevazioni sull'eventuale aumento del traffico generale telefonico e sull'eventuale aumento dell'importo delle bollette. In caso di riscontro positivo si procederà (secondo quanto previsto dal punto precedente) ad analizzare il costo totale dei singoli numeri telefonici. Solo successivamente a questa verifica potranno essere presi provvedimenti disciplinari.

5.7 - Garanzie per il lavoratore

Amia Spa assume l'impegno di non accedere ai dati inerenti al traffico telefonico per finalità diverse da quella della tutela del patrimonio aziendale.

6 - SOGGETTI COINVOLTI

Ai Responsabili del Trattamento dei Dati e agli appartenenti al Reparto Sistemi Informativi (EDP) sono state impartite precise istruzioni sul tipo di controlli ammessi e sulle relative modalità.

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, sarà posta opportuna cura nella prevenzione di accessi illegittimi a dati personali presenti in cartelle o spazi di memoria.

I soggetti preposti al trattamento dei dati (in particolare, gli incaricati della manutenzione) svolgeranno solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

In particolare, per le operazioni effettuate in assistenza remota necessarie data la dislocazione sul territorio dell'hardware aziendale, il personale incaricato avviserà preventivamente l'utente del singolo PC prima della connessione da remoto ed a operazioni concluse.

I soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi sono edotti e consapevoli delle linee di condotta da tenere, attraverso un'adeguata attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

6.1 - Responsabili del Trattamento

Giampaolo Tessari

Luca Mantovani

Graziella Santagati

6.2 - Amministratori di sistema

Gaetano Marchesini

Luca Mantovani

6.3 - Fiduciari

Giampietro Cigolini

Gianluigi Damiani

Mauro Bonato

Gaetano Marchesini

Franco Ferrari

Diego Testi

Giampaolo Tessari

Luca Mantovani

Graziella Santagati

Marco Durante

Andrea Friso

Moreno Pensa

Roberto Prati

Daniele Fretti

7 - SANZIONI

AMIA SpA si riserverà di adottare adeguati provvedimenti, anche di tipo disciplinare, qualora si constati un utilizzo degli strumenti aziendali contrario a quanto previsto dal presente regolamento, secondo le modalità previste all'art. 7 dello Statuto dei Lavoratori, dal Contratto Collettivo Nazionale di Lavoro e dal Codice Civile (artt. 2104 – 2105).

Le sanzioni disciplinari saranno graduate a seconda della gravità del comportamento punito, partendo dalla più lieve, il rimprovero verbale, fino alla possibilità di licenziamento senza preavviso.

Per il C.C.N.L. Federambiente le sanzioni previste sono le seguenti:

- rimprovero verbale
- rimprovero scritto
- multa fino a quattro ore di normale retribuzione;
- sospensione dal lavoro e dalla retribuzione da 1 a 10 giorni;
- licenziamento con preavviso
- licenziamento senza preavviso

8 - DISPOSIZIONI GENERALI

E' fatto espresso divieto di comunicare all'esterno qualunque notizia appresa all'interno dell'azienda che possa recare pregiudizio allo svolgimento della sua attività.

Questo documento è destinato esclusivamente ad un uso interno ad AMIA SpA.

Pertanto si fa espresso divieto a chiunque ne venga in possesso di diffonderlo all'esterno della stessa. La sua diffusione esterna potrà avvenire solo ed esclusivamente previa autorizzazione scritta.

AMIA SpA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Deliberazioni - 01 marzo 2007

Bollettino del n. 81/marzo 2007, pag. 0

[doc. web n. 1387522]

Lavoro: le linee guida del Garante per posta elettronica e internet
Gazzetta Ufficiale n. 58 del 10 marzo 2007

Registro delle deliberazioni
Del. n. 13 del 1° marzo 2007

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visti i reclami, le segnalazioni e i quesiti pervenuti riguardo ai trattamenti di dati personali effettuati da datori di lavoro riguardo all'uso, da parte di lavoratori, di strumenti informatici e telematici;

Vista la documentazione in atti;

Visti gli artt. 24 e 154, comma 1, lett. b) e c) del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Mauro Paissan;

PREMESSO

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

1.1. *Premessa*
Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.

Occorre muovere da alcune premesse:

a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (*artt. 15, 31 ss., 167 e 169 del Codice*);
c) emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
d) l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di *log file* della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi,

identificati o identificabili. (1)

1.2. *Tutela del lavoratore*
Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà. (2)

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (*artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato*). (3)

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. *Principi generali*
Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (*artt. 1 e 2 del Codice*). Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. *Discipline di settore*
Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (*artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300*).

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (*art. 47, comma 3, lett. b) Codice dell'amministrazione digitale*). (4)

2.3. *Principi del Codice*
I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

a) il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (*art. 3 del Codice; par. 5.2*);
b) il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, comma 1, lett. a), del Codice*). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (*v. par. 3*);
c) i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art. 11, comma 1, lett. b), del Codice: par. 4 e 5*), osservando il principio di *pertinenza* e *non eccedenza* (*par. 6*). Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti (*par. 8*) ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (*Parere n. 8/2001, cit., punti 5 e 12*).

3. Controlli e correttezza nel trattamento

3.1. *Disciplina interna*
In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (*art. 4, secondo comma, Statuto dei lavoratori;allegato VII, par. 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico "all'insaputa dei lavoratori"*). (5)

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali

siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. *Linee guida*
In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il *download* di *software* o di *file* musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime -specifiche e non generiche- per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (*art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10*).

3.3. *Informativa (art. 13 del Codice)*
All'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2..

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati (*art. 4, secondo comma, l. n. 300/1970*); possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (*art. 11, comma 1, lett. b), del Codice*), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (*cfr. artt. 2086, 2087 e 2104 cod. civ.*).

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (*art. 4, primo comma, l. n. 300/1970*), tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica.

Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli. (6)

In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire -a volte anche minuziosamente- l'attività di lavoratori. É il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di computer portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. (7) A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (*art. 11, comma 2, del Codice*). (8)

5. Programmi che consentono controlli "indiretti"

5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (*art. 4, comma 2*), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. (9) Ciò, anche in presenza di attività di controllo discontinue. (10)

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati (11), nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. (12)

5.2. *Principio di necessità*
In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure "repressive") e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori *(artt. 3, 11, comma 1, lett. d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4)*.

Dal punto di vista organizzativo è quindi opportuno che:

- si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet; (13)
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure *tecnologiche* volte a minimizzare l'uso di dati identificativi (c.d. *privacy enhancing technologies-PETs*). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).

a) Internet: la navigazione web
Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (*art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv. 2 febbraio 2006, cit.*).

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni -reputate inconferenti con l'attività lavorativa- quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) Posta elettronica
Il contenuto dei messaggi di posta elettronica -come pure i dati esteriori delle comunicazioni e i *file* allegati- riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (*artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale*). (14)

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una *policy* al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita").

É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore; (15)
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. (16) In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

6. Pertinenza e non eccedenza

6.1. *Graduazione dei controlli*
Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni

elettroniche di natura personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. *Conservazione*
I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario -e predeterminato- a raggiungerla (*v. art. 11, comma 1, lett. e), del Codice*).

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. *Datori di lavoro privati*
I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (*v., in particolare, art. 4, secondo comma, dello Statuto*), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.

Ciò, può avvenire:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (*art. 24, comma 1, lett. f) del Codice*);
b) in caso di valida manifestazione di un libero consenso;
c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (*art. 24, comma 1, lett. g), del Codice*).

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).

L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

7.2. *Datori di lavoro pubblici*
Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (*artt. 18-22 e 112*).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (*art. 7, comma 4, lett. a), del Codice*).

8. Individuazione dei soggetti preposti

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (*art. 29 del Codice*).

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.

Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9).

TUTTO CIÒ PREMESSO IL GARANTE

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:

a) l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);

b) l'adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:

- si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
- si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;

c) l'adozione di misure di tipo tecnologico, e segnatamente:

I. rispetto alla "navigazione" in Internet (punto 5.2., a):

- l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
- la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
- il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
- l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
- la graduazione dei controlli (punto 6.1.);

II. rispetto all'utilizzo della posta elettronica (punto 5.2., b):

- la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
- l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
- la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di

apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;

- consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- la graduazione dei controlli (punto 6.1.);

3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:

a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;

b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;

c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

d) l'analisi occulta di computer portatili affidati in uso;

4) individua, ai sensi dell'art. 24, comma 1, lett. g), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;

5) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 1° marzo 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

---

(1) Cfr. Gruppo Art. 29 sulla protezione dei dati, Parere n. 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione, 13 settembre 2001, punti 5 e 12, in http://ec.europa.eu/...pdf.

(2) Cfr. Niemitz v. Germany, 23 novembre 1992, par. 29; v. pure Halford v. United Kingdom, 25 giugno 1997, parr. 44-46.

(3) V. pure Gruppo Art. 29 cit., Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, Wp 55, 29 maggio 2002, p. 4, in http://ec.europa.eu/...pdf.

(4) V. pure la Direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni del 27 novembre 2003; Raccomandazione n. R (89)2 del Consiglio d'Europa in materia di protezione dei dati personali nel contesto del rapporto di lavoro, in http://cm.coe.int/...doc); Parere n. 8/2001 , cit., punto 5.

(5) V. altresì la Raccomandazione n. R (89) 2, cit., punto 3; Parere n. 8/2001 , cit., punto 9.1 e Wp 55, cit., punto 3.1.3.

(6) Cass. 18 febbraio 1983, n. 1236 e 16 settembre 1997, n. 9211.

(7) Cfr. Cass. 11 marzo 1986, n. 1490.

(8) Cfr. anche Cass., 17 giugno 2000, n. 8250 rispetto all'uso probatorio.

(9) Cass. 18 febbraio 1983, n. 1236 e 16 settembre 1997, n. 9211.

(10) Cass. 11 marzo 1986, n. 1490 cit.

(11) Raccomandazione n. R (89)2, cit., art. 3, comma 1.

(12) Raccomandazione n. R (89)2, art. 3, comma 2; disposizione in base alla quale, in presenza di rischi "per il diritto al rispetto della vita privata e della dignità umana dei lavoratori, dovrà essere ricercato l'accordo dei lavoratori o dei loro rappresentanti prima dell'introduzione o della modifica di tali sistemi o procedimenti, a meno che altre garanzie specifiche non siano previste dalla legislazione nazionale": art. 3, comma 3.

(13) Cfr. Provv. 2 febbraio 2006 , in *http://www.garanteprivacy.it*, doc. web n. 1229854.

(14) Cfr. nota del Garante 16 giugno 1999 , Boll. n. 9, giugno 1999 , p. 96; Tar Lazio, Sez. I ter, 15 novembre 2001, n. 9425.

(15) Cfr. il documento Wp 55, cit., p. 23.

(16) Cfr. il documento Wp 55, cit., p. 5.

stampa **chiudi**

AMIA Verona S.p.a.
Prot. N. 9782/08
del 20.08.2010

Spettabili R.S.A.

F.P. - C.G.I.L.
F.I.T. - C.I.S.L.
U.I.L. Trasporti
C.I.S.A.L. Enti Locali e Servizi
U.G.L.

S e d e

OGGETTO: Incontro Sindacale.

I Rappresentanti delle RSA in indirizzo sono invitati ad un incontro che si terrà

MERCOLEDI' 1 SETTEMBRE 2010 - alle ore 9.00
presso la sede aziendale di Via B. Avesani, 31

Ordine del giorno:

- **Obiettivi 2010;**
- **Recepimento Policy aziendale;**
- **Buoni pasto;**
- **Varie ed eventuali.**

Cordiali saluti.

IL DIRETTORE GENERALE
(Ing. Giampietro Cigolini)