ALTAVITA-ISTITUZIONI RIUNITE DI ASSISTENZA-I.R.A.

Regolamento per l'utilizzo della Posta elettronica e di Internet nel posto di lavoro

INDICE

1. Premessa

Il Garante con provvedimento generale del 1° marzo 2007 pubblicato nella G.U. n. 58 del 10 marzo 2007 stabilisce che i datori di lavoro pubblici e privati individuano preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet.

I datori di lavoro sono altresì tenuti ad adottare delle misure per conformare alle disposizioni vigenti il trattamento di dati personali al fine di verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.

Il presente regolamento rientra ed estende le azioni di tutela verso il personale dipendente dato che le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su di un computer, ma nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

Questi atteggiamenti sorreggono ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

2. Definizioni

a) **"dato personale"**, 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;
b) **"dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;
c) **"dati sensibili",** i dati personali 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 od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
d) **"dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei

relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

e) **"incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
f) **"interessato",** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
g) **"comunicazione"**, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
h) **"diffusione"**, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
i) **"dato anonimo"**, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
j) **"blocco"**, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
k) "**banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

3. Il trattamento dei dati personali

Il trattamento dei dati personali compresi quelli del personale dipendente effettuato dall'Istituto comprende qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti:

a) la raccolta;
b) la registrazione cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
c) l'organizzazione;
d) la conservazione;
e) la consultazione;
f) l'elaborazione;
g) la modificazione;
h) la selezione;
i) l'estrazione;
j) il raffronto;
k) l'utilizzo;
l) l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
m) il blocco, ovvero la conservazione dei dati con sospensione temporanea di ogni altra operazione di trattamento;
n) la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
o) la diffusione, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

p) la cancellazione;
q) la distruzione di dati;

4. Prescrizioni generali su come deve avvenire il trattamento dei dati

L'Istituto garantisce che i dati personali oggetto di trattamento siano:

a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi, ed in ogni caso nei limiti in cui il trattamento sia necessario per il funzionamento della nostra organizzazione;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

5. I sistemi informatici

Le tecnologie dell'informazione permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, a volte anche all'insaputa o senza la piena consapevolezza del personale, considerate anche le potenzialità della tecnologia e la dimensione dei rischi connessi all'uso di internet e della posta elettronica. Il presente regolamento stabilisce le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette, e in che misura e con quali modalità vengano effettuati controlli.

I trattamenti dei dati personali effettuati dall'Istituto rispettano le garanzie in materia di protezione dei dati stessi e in particolare di quelli del personale e si svolgono osservando i seguenti principi:

a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi in relazione alle finalità perseguite;

b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti vengono rese note ai lavoratori;

c) il principio di pertinenza e non eccedenza, secondo cui i trattamenti sono effettuati per finalità determinate, esplicite e legittime. I dati sono trattati nella misura meno invasiva compatibile con lo stato dell'arte della tecnologia informatica; le attività di monitoraggio sono svolte solo da soggetti preposti e sono *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, del principio di segretezza della corrispondenza"*.

Al fine di garantire i principi di cui ai punti precedenti e per assicurare la massima protezione dei dati personali dei dipendenti, è necessario che siano rispettate da parte del personale dipendente dell'Istituto le seguenti indicazioni:

- le apparecchiature informatiche (personal computer, stampanti, periferiche in genere) sono strumenti di lavoro affidati al dipendente e vanno custoditi in modo appropriato nonché utilizzati solo per fini professionali ed in relazione, alle mansioni assegnate;
- onde evitare il pericolo di introduzione di programmi non autorizzati finalizzati alla comunicazione di dati personali è consentito installare programmi provenienti dall'esterno, solo se espressamente autorizzati;
- non è consentito utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito modificare le configurazioni impostate sulla propria postazione di lavoro;
- non è consentita l'installazione sulla propria postazione di lavoro di mezzi di comunicazione personali o modalità di accesso verso l'esterno della rete dell'ente se non espressamente concordato e autorizzato dal responsabile per la sicurezza;
- non è consentito in genere l'uso delle periferiche della postazione di lavoro se non ai fini prettamente lavorativi;
- non è ammesso l'uso in genere delle risorse informatiche per l'archiviazione di documenti personali (documenti, programmi, immagini, audio, video, archivi in genere, etc). Casi particolari devono essere espressamente autorizzati dalla direzione dei sistemi informativi.

Per le attività connesse, all'accesso al sistema informatico ci si deve attenere alle seguenti disposizioni:

- **utilizzare direttamente le credenziali personali assegnate** per accedere alle procedure informatiche e non comunicare a nessuno le credenziali assegnate (nome utente e password);
- **non consentire l'accesso a terzi, nessuno escluso**, alla apparecchiatura informatica con le proprie credenziali di autenticazione e non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- **non utilizzare credenziali (user-id e password) di altri utenti**, nemmeno se fornite volontariamente o di cui si è casualmente a conoscenza;
- **non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione** a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;
- **è fatto obbligo di adottare le necessarie cautele per assicurare la segretezza delle credenziali assegnate** (nome utente e password). La perdita o la venuta a conoscenza di utilizzo da parte di altri delle proprie credenziali deve essere comunicata al Responsabile della Sicurezza il quale provvederà al rilascio di nuove e sostitutive modalità di autenticazione al sistema informatico;
- **nei casi di prolungata assenza o impedimento del dipendente**, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password del dipendente stesso, per accedere agli strumenti ed ai dati. A tale fine, la direzione dei sistemi informativi procede a rigenerare una nuova password, diversa da quella in uso al

dipendente assente, che verrà utilizzata per l'accesso. La richiesta di accesso per il caso descritto, opportunamente motivata, deve essere formalmente inoltrata al Servizio Informatico da parte del responsabile del servizio competente anche via e-mail;
- dell'eventuale accesso, in caso di assenza, verrà data al dipendente tempestiva comunicazione e si provvederà a sostituire ed assegnare un nuova parola chiave.

6. Categorie di dipendenti abilitati all'utilizzo di Internet e del sistema di Posta elettronica

Per quanto riguarda la Posta Elettronica l'Istituto stabilisce, anche in adempimento al Codice dell'Amministrazione Digitale, che la Posta Elettronica sia uno degli strumenti strategici in ordine ai rapporti con i propri utenti e i propri fornitori nonché finalizzato alla maggiore efficienza delle relazioni interne.

Pertanto ai dipendenti, coinvolti direttamente o indirettamente nei procedimenti amministrativi, viene assegnata una casella di posta elettronica ad uso aziendale.

Parimenti, i servizi e settori dell'Istituto, fanno riferimento ad una casella di posta elettronica istituzionale.

7. Navigazione in Internet

Non è consentito navigare in siti non attinenti lo svolgimento delle mansioni assegnate soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente.

Non è consentita l'effettuazione di ogni genere di transazione finanziaria, comprese le operazioni di remote banking, acquisti on line e simili, salvo i casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto.

Non è consentito lo scarico di software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato.

Non è consentito lo scarico di file musicali, film, multimediali in genere se non espressamente autorizzati o pertinenti la propria mansione lavorativa. Non è neppure consentito detenere nelle unità di rete o dischi della postazione di lavoro documenti del genere indicato anche se non provenienti da Internet.

E' vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa, né è permessa la partecipazione per motivi non professionali a Forum, l'utilizzo di Chat Line, di Bacheche Elettroniche e le registrazioni in guestbook (anche utilizzando pseudonimi o nicknames).

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

E' consentita la navigazione solo in siti correlati con le attività, i procedimenti e le relazioni istituzionali dell'Istituto. (Per esempio siti delle amministrazioni centrali e periferiche dello stato, sanità, regioni, province, comuni, comunità locali, autorità giudiziaria, siti previdenziali e assistenziali, fornitori, provider, enti economici, centri servizi, etc…).

8. Disposizioni relative all' utilizzo del sistema di Posta Elettronica

Non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate.

Non è consentito inviare, memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti riservati.

Ogni comunicazione (interna ed esterna), inviata o ricevuta, che abbia contenuti rilevanti o contenga impegni deve essere visionata od autorizzata dal responsabile del servizio.

Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o Mail-List, salvo diversa ed esplicita autorizzazione.

Le caselle di posta elettronica dell'Istituto sono definite e assegnate in conformità delle indicazioni del Codice dell'Amministrazione Digitale e precisamente sono presenti caselle di posta elettronica istituzionali e caselle di posta elettronica associate alle posizioni di lavoro del personale.

Le comunicazioni di riferimento avvengono tra caselle di posta elettronica istituzionale, i responsabili delle caselle di posta elettronica istituzionale interessano di volta in volta a seconda delle necessità del procedimento amministrativo e dei compiti assegnati, le caselle di posta assegnate alle varie posizioni di lavoro. Le caselle di posta elettronica assegnate alle varie posizioni di lavoro sono da considerarsi a tutti gli effetti caselle di posta elettronica aziendali.

Le posizioni di lavoro comunicano prioritariamente con la casella di posta elettronica istituzionale di riferimento, fatto salvo direttive diverse da parte del responsabile del servizio.

Sono temporaneamente memorizzate le tracce delle comunicazioni in registri denominati file di log.

Ciò al fine di garantire una corretta gestione e le azioni di controllo finalizzate ad evitare

comunicazioni indesiderate. L'accesso ai soli fini della garanzia dell'efficacia delle misure minime di sicurezza adottate in adempimento al D.Lvo 196/2003 è abilitato alla direzione dei sistemi informativi. Gli accessi alle procedure di controllo di diagnosi di eventuali anomalie sono esclusivamente di natura interna e in forma assolutamente anonima. Dette registrazioni sono conservate solo per il tempo necessario al raggiungimento del buon fine delle comunicazioni e sono regolarmente eliminate o soprascritte.

L'Istituto si riserva la facoltà di effettuare controlli in conformità alla legge, anche saltuari o occasionali, qualora si verifichino condizioni di attacco informatico, di malfunzionamenti segnalati, di necessità di aumentare i livelli delle misure di sicurezza e di verifica negli abusi nell'utilizzo.

Qualora si verifichino le condizioni citate sarà cura della direzione dei sistemi informatici emettere comunicati collettivi o individuali.

Potranno essere attivate apposite funzionalità di sistema, di agevole utilizzo, che consentono di inviare automaticamente, in caso di assenze (per esempio, 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.

In caso di eventuali assenze non programmate (ad esempio, per malattia), qualora il dipendente non possa attivare la procedura descritta, il responsabile dei servizi informativi su richiesta del responsabile del servizio, perdurando l'assenza oltre un determinato limite temporale, potrà lecitamente disporre, l'attivazione di un procedimento di accesso alla casella di posta elettronica individuale per l'attivazione del servizio di cui al comma precedente, previo avvertimento all'interessato.

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 della casella assegnata al dipendente, ogni dipendente comunica al proprio responsabile del servizio il nominativo di un altro dipendente delegato e fiduciario, che procede a verificare il contenuto di messaggi e a inoltrare al responsabile del servizio quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Se si verifica la condizione di accesso alla casella di posta elettronica assegnata al dipendente, da parte del delegato o fiduciario, il responsabile del servizio provvede a redigere apposito verbale ed a informare il dipendente interessato alla prima occasione utile.

Potranno essere definiti, nei messaggi di posta elettronica, delle frasi che conterranno 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.

9. Conservazione

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente, attraverso procedure di sovraregistrazione, i registri delle attività generati dai programmi informatici di gestione dei sistemi di posta elettronica e dei programmi informatici che permettono l'accesso ad Internet.

I tempi di conservazione dei registri di attività sono determinati in un tempo massimo di 12 mesi, dopo i quali, detti registri vengono soprascritti. L'accesso alle registrazioni ha luogo solo in relazione:

- ad esigenze tecniche o di sicurezza;
- 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.

10. Controlli

I controlli sono obbligatori per legge in adempimento degli artt. 31-35 e del disciplinare tecnico Allegato B) D.Lvo 196/2003, al fine di attuare le procedure di protezione dei dati personali contro il rischio di intrusione ai sensi dell'art. 615 ter del codice penale nonché contro il rischio dell'azione di programmi di cui all'art. 615-quinquies del codice penale.

Nell'effettuare detti controlli sull'uso degli strumenti elettronici, viene accuratamente evitata qualsiasi 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. Detti controlli rispettano i principi di liceità, pertinenza e non eccedenza.

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

Il controllo è preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Non è ammessa e quindi esclusa la condizione di controlli prolungati, costanti o indiscriminati.

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.

11. Responsabilità

L'utente è responsabile di qualsiasi danno arrecato in dipendenza della mancata osservazione di quanto previsto dal presente regolamento.

L'utente può essere chiamato a rispondere civilmente, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e/o password, con particolare riferimento all'immissione in rete di contenuti non ammessi o in genere in contrasto con la legislazione italiana.

La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente Contratto di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità penale.

12. Misure di sicurezza adottate

Le misure di sicurezza che sono state adottate al fine di assicurare il più alto livello di disponibilità, integrità e riservatezza del sistema di posta elettronica e del sistema di accesso alla rete internet sono i seguenti:

- apparati che provvedono alla ricezione e invio di posta elettronica contrastando messaggi indesiderati e applicando livelli commisurati di protezione dalle vulnerabilità conosciute sia sui messaggi che sugli allegati;

- apparati di configurazione di un particolare sistema di web blocking, che tende a restringere il campo di consultazione ai soli web-site che sono stati definiti come "pertinenti" ed "utili". Ogni utente che dia vita ad una sessione di browsing internet, sarà soggetto al vaglio di questo servizio di web-blocking, il quale comunicherà in risposta l'assenso o il diniego all'apertura della specifica pagina web.

13. Disposizioni finali

Il presente regolamento costituisce estensione e integrazione delle informative dovute ai sensi dell'art. 13 del D.Lvo 196/2003.

L'Istituto nella sua azione costante, anche in relazione alle conoscenze acquisite in base al progresso tecnico, tesa al miglioramento delle misure di sicurezza al fine di ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme, si riserva di emanare ulteriori disciplinari interni, destinati agli incaricati, con i quali sono dettate le regole generali di comportamento nell'uso della strumentazione elettronica e non per tutti i trattamenti di dati connesse alle funzioni e alle competenze istituzionali.