DIRETTIVA PER L'UTILIZZO DELLA POSTA ELETTRONICA E DI INTERNET PRESSO IRPET

Indice generale

Premessa

Negli ultimi anni l'organizzazione del lavoro è stata sottoposta ad un imponente processo di informatizzazione; in tale contesto i servizi di rete, tra cui posta elettronica ed internet, sono diventati strumenti quotidiani indispensabili per l'esercizio dell'attività lavorativa dal momento che consentono l'immediatezza, la democratizzazione e la trasversalità dell'informazione.

Poiché le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi, l'utilizzo delle risorse informatiche messe a disposizione del personale deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti richiesti nello svolgimento di ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, in qualsiasi forma esso sia.

La protezione dei dati e delle informazioni nel loro complesso è condizione necessaria per garantire il rispetto dei requisiti di sicurezza che la normativa vigente impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di dati personali.

Il datore di lavoro, inoltre, deve assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori.

La presente direttiva persegue le seguenti finalità:

- adottare indirizzi trasparenti, capaci di comunicare con estrema chiarezza al lavoratore le corrette modalità di utilizzo degli strumenti informatici assegnatigli per lo svolgimento delle mansioni attribuite,
- definire con altrettanta chiarezza il diritto dell'Ente datore di lavoro a verificare l'uso corretto dei suddetti strumenti,
- individuare le modalità con cui l'Ente esercita tale diritto di verifica.

La presente direttiva è diretta anche ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati.

Art. 1
Contesto normativo

I principi applicati nella stesura della direttiva sono tratti dal quadro normativo che segue:

Art. 15 Costituzione

Norme del codice civile: artt. 2087, 2104, 2105 e 2106.

L. 20 maggio 1970, n. 300 (Statuto dei lavoratori) - artt. 4 e 8.

D.lgs. del 9 aprile 2008 n. 81. in materia di sicurezza sul lavoro.

Codice in materia di protezione dei dati personali (D. Lgs. n. 196/2003).

Art. 49, D.Lgs. 7 marzo 2005 n. 82, Codice dell'amministrazione digitale, "Segretezza della corrispondenza trasmessa per via telematica".

"`Linee guida del Garante per posta elettronica e internet", emanate con deliberazione l marzo 2007 n. 13.
“Misure e accorgimenti prescritti relativamente alle attribuzioni delle funzioni di amministratore di sistema e soggetti preposti ad attività riconducibili alle mansioni tipiche dei c.d. “amministratori di sistema” (provvedimento del Garante in G.U. n.300 del 24 dicembre 2008.
Direttiva n° 02/2009 P.C.M. “Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro”

Art. 2
Ambito di applicazione

L'ambito in cui intende muoversi la direttiva è quello relativo all'individuazione di regole comuni per tutelare i reciproci diritti e doveri di lavoratori e datore di lavoro attraverso la definizione:

- delle modalità per l'utilizzo e l'accesso al servizio internet e di posta elettronica da parte dei dipendenti dell'IRPET e di tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture dell'IRPET;
- del diritto dell'IRPET di verificare che non avvengano usi impropri;
- del diritto del lavoratore (e dei terzi) ad una sfera di riservatezza anche nelle relazioni lavorative.

Le prescrizioni contenute si aggiungono e integrano le norme già previste dal contratto collettivo nazionale di lavoro, nonché dalla normativa in materia di protezione dei dati personali (D.Lgs. 196/2003).

Art. 3
Titolarità degli strumenti e delle apparecchiature informatiche

L'IRPET (di seguito indicato anche come 'Istituto') è proprietario degli strumenti e delle apparecchiature informatiche assegnati ai dipendenti o collaboratori. Tali strumenti sono affidati ai medesimi a condizione che vengano custoditi con cura, evitando manomissioni, danneggiamenti o utilizzi per scopi non consentiti, anche da parte di altre persone. E' precipuo dovere dell'affidatario predisporre le idonee misure atte a evitare intrusioni o manomissioni da parte di soggetti terzi alle attrezzature affidate.

Art. 4

Conformità alla legge

Le risorse informatiche fornite dall'IRPET devono essere utilizzate unicamente per perseguire gli scopi lavorativi.
I dipendenti ed i collaboratori dell'IRPET sono tenuti a rispettare la legge e la normativa regionale in materia nonché le eventuali disposizioni di volta in volta emanate dall'IRPET.

Art. 5

Rispetto della proprietà intellettuale e delle licenze

Tutto il personale dell'IRPET è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale e non può, sulle apparecchiature fornite ai sensi dell'art. 3, installare hardware o software né duplicare o utilizzare software che non sia stato preinstallato, installato o comunque fornito dall'IRPET.

Art. 6

Utilizzo dei dati e del software

I dati e le informazioni sono beni dell'Istituto.
I dati e le informazioni detenute su apparecchiature dell'Istituto o altri supporti sono utilizzati dal personale, anche fuori dagli uffici dell'IRPET, ai soli fini lavorativi.
Nessun dato dell'Istituto o personale può essere trattato o memorizzato su dispositivi elettronici di qualsiasi tipologia, non finalizzati all'attività lavorativa.
I dati e le informazioni memorizzate, elaborate e/o comunicate attraverso le apparecchiature informatiche in uso presso l'Istituto possono essere in qualsiasi momento oggetto di controllo da parte dell'IRPET per esigenze legate a motivi di sicurezza o controllo di spesa o efficienza e manutenzione dei servizi.

Art. 7

Utilizzo della Posta elettronica

Il servizio di posta elettronica erogato dai sistemi dell'Istituto è ad uso esclusivo di IRPET.
L'assegnazione delle caselle di posta elettronica ai dipendenti è finalizzata all'utilizzo di tale mezzo di comunicazione per lo svolgimento dell'attività lavorativa.
Ogni comunicazione via posta elettronica con soggetti esterni od interni all'IRPET

deve avvenire esclusivamente mediante l'utilizzo del sistema di posta elettronica dell'Istituto, per garantire i necessari livelli di sicurezza e riservatezza.
Non sono consentiti gli utilizzi finalizzati a divulgare contenuti illeciti o altrimenti inaccettabili, oppure finalizzati a violare i diritti legali altrui.
Al dipendente è vietato intercettare, alterare, impedire o interrompere comunicazioni di altri utilizzatori della rete ed installare apparecchiature idonee a tale scopo, salvo che queste attività non siano atte a garantire le previste misure di sicurezza.

Art. 8
Utilizzo di internet

Il collegamento a internet, reso disponibile sulle postazioni di lavoro, è finalizzato all'utilizzo di tale mezzo di comunicazione per lo svolgimento dell'attività lavorativa.

Art. 9
Monitoraggio e controlli

A garanzia della sicurezza dei sistemi informativi e dei servizi di rete, è nella facoltà dell'IRPET effettuare controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree, nonché predisporre controlli a campione, in forma anonima, sugli accessi ad internet e sulla navigazione web.
È sempre fatta salva l'ipotesi dell'attivazione di controlli, anche individualizzati, che trovino giustificazione nella necessità di corrispondere ad eventuali richieste di organi di polizia su segnalazione dell'autorità giudiziaria, nel verificarsi di un evento dannoso o di una situazione di pericolo che richieda un immediato intervento o nella presenza di sospetti relativamente all'esistenza di condotte improprie nell'uso delle apparecchiature (c.d. controlli difensivi).
L'IRPET non effettuerà trattamenti di dati personali mediante sistemi hardware e/o software che mirino al controllo a distanza dei lavoratori quali:

- lettura e/o 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;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore.

L'Istituto è dotato di un sistema di filtraggio dei contenuti accessibili via internet, che preclude l'accesso a determinate categorie di risorse per la loro non attinenza alle attività istituzionali e per garantire a tutti la fruibilità e la sicurezza di internet. Nella configurazione attuale sono banditi i siti rientranti nelle seguenti categorie (secondo la classificazione del fornitore):

- Acquisti → Aste/annunci
- Armi/militari
- Criminalità → Attività illegali
- Criminalità → Estremismo politico/Odio/Discriminazione
- Criminalità → warez / criminalità informatica
- Divertimento/cultura → Musica/radio
- Giochi/gambling
- Informazione/comunicazione → cartoline digitali
- Malware
- Pornografia/nudità
- Spam
- Tecnologia informatica → anonymous proxies
- Violenza / siti estremi

Parallelamente alle categorie sopraelencate sono attive una lista di siti comunque ammessi (indipendentemente dalla classificazione) e una lista di siti comunque banditi; l'inserimento di siti in una delle due liste può essere ottenuto dai dipendenti mediante richiesta motivata all'Amministratore di sistema.
La politica generale di filtraggio dei contenuti web è orientata principalmente a preservare risorse condivise e scarse (la banda di trasmissione dati) e non a precludere l'accesso a determinate categorie di contenuti
Nei casi di accertata violazione dei principi fissati nel presente disciplinare, è demandata al dirigente responsabile di ciascuna struttura organizzativa dell'IRPET l'avvio delle procedure disciplinari individuate nel CCNL, con le modalità ivi previste per il personale dipendente o equiparato, ovvero l'applicazione delle sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti.

Art. 10
Amministratore di sistema

L'Amministratore di sistema designato dall'Istituto ai sensi del codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n° 196) e del provvedimento del garante del 24 dicembre 2008, n° 300 si occupa di:

- implementare e assicurare la manutenzione in efficienza delle postazioni di lavoro e dei servizi informatizzati forniti dall'Istituto;
- implementare le misure atte a garantire la sicurezza e l'integrità delle risorse informatiche dell'Istituto (software, hardware, dati);

Nell'esercizio dei suoi compiti l'Amministratore di sistema può in qualsiasi momento avere la necessità di accedere alle postazioni di lavoro, alle caselle di posta elettronica e ai dati su server di dipendenti e collaboratori; questo di norma avverrà sempre alla presenza della persona interessata (assegnataria della postazione e titolare della casella di posta elettronica e/o dei dati) e comunque previa notifica; la persona interessata può richiedere di far presenziare all'attività un dipendente o collaboratore

di sua fiducia previamente individuato mediante atto scritto e custodito presso il servizio Amministrazione dell'Istituto.
L'Amministratore di sistema può inoltre svolgere attività di monitoraggio della posta elettronica e del flusso dati attraverso la rete dell'Istituto, in forma occasionale e non sistematica, finalizzata alla ricerca di eventuali minacce alla sicurezza o anomalie nel funzionamento dei servizi che si dovessero verificare, senza dovere dare preavviso della propria attività.