



COMUNE di PAVIA

N° 198 Reg. Delib.

DELIBERAZIONE DELLA GIUNTA COMUNALE

OGGETTO: Linee guida per l'utilizzo degli strumenti informatici, di Internet e della posta elettronica

L'anno 2011 il giorno 20 del mese di dicembre nella consueta sala delle adunanze si è riunita la Giunta Comunale sotto la presidenza del Sindaco Alessandro Cattaneo per deliberare sull'oggetto su indicato.

Sono presenti i Signori:

Sindaco: Alessandro Cattaneo
Assessori: Assanelli
Bobbio Pallavicini
Bruni
Centinaio
Fracassi
Galandra
Niutta
Valdati

Sono assenti i Signori:

Faldini
Greco

Partecipa ed assiste il Segretario Generale del Comune dott. Pietro Paolo Mileti.

Constatato il numero legale degli intervenuti, il Presidente pone in trattazione l'oggetto su indicato.

LA GIUNTA COMUNALE

Su relazione del Sindaco,

premessi che:

- le risorse ICT (Information and Communication Technology) costituiscono, ormai da tempo, il principale strumento di lavoro posto a disposizione dei dipendenti delle pubbliche amministrazioni;
- l'ampia distribuzione di tali risorse tra i dipendenti ne favorisce il diffuso utilizzo anche per finalità diverse da quelle strettamente lavorative;

Tenuto conto che le Pubbliche Amministrazioni, in quanto datori di lavoro, sono tenute ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi.

Preso atto che:

- la direttiva 2/09 del Dipartimento della Funzione Pubblica invita le Pubbliche Amministrazioni ad adottare tutte le misure di informazione, controllo e verifica consentite al fine di regolamentare la fruizione delle risorse ICT e responsabilizzare i dipendenti nei confronti di eventuali utilizzi non coerenti con la prestazione lavorativa e non conformi alle norme che disciplinano il lavoro alle dipendenze delle pubbliche amministrazioni;
- con deliberazione n. 13 del 1 marzo 2007 il Garante della protezione dei dati personali ha fornito le linee guida per l'utilizzo nei luoghi di lavoro della posta elettronica e di internet;

Valutato che è necessario contemperare l'utilizzo degli strumenti ICT con la protezione dei dati personali tenuto conto che come indicato nella Deliberazione del Garante per la Protezione dei dati personali n. 13 del 1° marzo 2007:

- 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;
- spetta ai datori di lavoro 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;
- 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 da vari strumenti di registrazione delle informazioni;
- i servizi di posta elettronica sono parimenti suscettibili di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

Rilevato per quanto sopra esposto che è opportuno adottare una policy interna rispetto al corretto uso degli strumenti informatici, della posta elettronica e Internet che indichi le modalità di utilizzo dei suddetti mezzi da parte dei lavoratori;

Dato atto che, sulla base delle disposizioni normative vigenti, è stato predisposto dagli uffici competenti l'allegato documento avente per oggetto "*Linee guida per l'utilizzo degli Strumenti*

Informatici, di internet e della posta elettronica” che, una volta approvato, andrà ad integrare il Documento Programmatico per la Sicurezza (DPS) di prossima approvazione;

Rilevato altresì che le linee guida formulate, oltre ad essere dettate dalla normativa vigente, rispondono agli indirizzi dell’Amministrazione in ordine all’utilizzo degli strumenti ICT, alla promozione dell’innovazione e alla progressiva informatizzazione dei procedimenti amministrativi nel pieno rispetto dei principi sul corretto utilizzo degli strumenti da parte dei dipendenti cui va garantita la tutela dei dati personali;

Dato atto che il presente provvedimento non comportando né impegno di spesa né diminuzione di entrata, non richiede il parere di regolarità contabile, espresso ai sensi dell’art. 49 del D. Lgs. 267/00, dal Dirigente responsabile dei Servizi Finanziari;

Acquisito il parere favorevole di regolarità tecnica espresso, ai sensi dell’art. 49 del D. Lgs. 267/00, dal Dirigente del settore Gestione Risorse umane e servizi Interni Dott.ssa Ivana dello Iacono allegato quale parte integrante e sostanziale al presente provvedimento;

Visto il D. Lgs. 267/2000 in particolare l’art. 48;

Visto lo Statuto Comunale;

Vista la normativa vigente in materia e il D. Lgs 196/2003 e s.m.i.

DELIBERA

1. le premesse costituiscono parte integrante e sostanziale del presente provvedimento;
2. di approvare, le *“Linee guida per l’utilizzo degli Strumenti Informatici, di internet e della posta elettronica”* secondo il testo allegato (Allegato A) al presente provvedimento di cui costituisce parte integrante e che consta di 24 articoli più allegati;
3. di dare atto che il documento costituirà parte integrante e sostanziale del Documento Programmatico della Sicurezza (DPS) per l’anno 2012.

Allegato alla delibera di Giunta Comunale
n. 198 del 20/12/2011



COMUNE DI PAVIA

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE N.

OGGETTO: Linee guida per l'utilizzo degli strumenti informatici, di Internet e della posta elettronica

SETTORE PROPONENTE: GESTIONE RISORSE UMANE E SERVIZI INTERNI

Si attesta che la proposta di deliberazione in oggetto è stata istruita da questo Settore

si esprime parere FAVOREVOLE, in ordine alla regolarità
tecnica, ai sensi dell'art. 49 del D. Lgs. n. 267 del 18.08.2000.

Pavia, li 16/12/2011

IL DIRIGENTE DEL SETTORE



Comune di Pavia

Allegato A

Si attesta che il presente documento composto di n. 34 pagine è allegato alla deliberazione della Giunta Comunale n. 138 in data 20/12/2014 della quale è parte integrante e sostanziale.

IL SEGRETARIO GENERALE

F. TO PIETRO POLO TILÈTI

Linee guida per l'Utilizzo degli Strumenti Informatici, di Internet e della Posta elettronica

Sommario

Capo 1 - Informazioni Generali	3
Art. 1 Principi generali	3
Art. 2 Definizioni	3
Art. 3 Finalità	3
Art. 4 Competenze e responsabilità.....	4
Art. 5 Titolarità.....	4
Capo 2 – Gli strumenti informatici	5
Art. 6 Acquisto di hardware e software.....	5
Art. 7 Rispetto della proprietà intellettuale e delle licenze	5
Art. 8 Utilizzo di hardware o software di proprietà personale	5
Art. 9 Utilizzo delle apparecchiature elettroniche.....	5
Art. 10 Utilizzo dei supporti magnetici.....	6
Art. 11 Utilizzo di dispositivi portatili e dei supporti per le presentazioni	7
Art. 12 Protezione dai virus.....	7
Capo 3 - La rete aziendale e Internet.....	7
Art. 13 Utilizzo della rete del Comune di Pavia	8
Art. 14 Gestione delle Password	8
Art. 15 Uso della rete Internet e dei relativi servizi	9
Capo 4 - La posta elettronica.....	10
Art. 16 Principi generali	10
Art. 17 Gestione del servizio.....	11
Art. 18 Gestione delle caselle di posta elettronica	11
Art. 19 Compiti e responsabilità	12
Art. 20 Utilizzazione del servizio.....	13
Art. 21 Pubblicità degli indirizzi	13
Capo 5 – Disposizioni finali.....	13
Art. 22 Violazioni.....	13
Art. 23 Aggiornamento e revisione	14
Art. 24 Disposizioni finali.....	14
Allegato A GLOSSARIO DEI TERMINI TECNICI E/O INFORMATICI.....	15
Allegato B Responsabilità per l'uso consentito del S.I.C.	21
Allegato C Modulo di richiesta	22
Allegato D Deliberazione del Garante Privacy n. 13 del 1° marzo 2007.....	24

Capo 1 - Informazioni Generali

Art. 1 Principi generali

1. La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet, espone il Comune di Pavia ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.
2. Tenuto conto quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, il Comune di Pavia con questo documento interno intende integrare e meglio esplicitare alcuni principi già contenuti nel Documento Programmatico per la Sicurezza approvato annualmente.
3. Tale ulteriore precauzione è volta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni che sono state fornite a tutti gli incaricati del trattamento in attuazione del D.lgs 196/03 - Testo Unico in materia di protezione dei dati personali.

Art. 2 Definizioni

1. Ai fini del presente documento si intende per:
 - a) "*Sistema Informativo del Comune di Pavia*" l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, software, archivi dati e/o risorse informative e di telecomunicazione a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Amministrazione Comunale di Pavia;
 - b) "*utente*", qualunque soggetto sia esso dipendente, collaboratore, amministratore o quant'altro che abbia titolo ad utilizzare la rete informatica o di telecomunicazioni Comunale ed i servizi da essa erogati.
2. Al fine di consentire una più agevole comprensione dei termini prettamente tecnici e/o informatici contenuti nel presente documento, si rinvia al glossario di cui all'allegato A.

Art. 3 Finalità

1. Le apparecchiature informatiche, di telecomunicazione, i programmi e tutte le varie funzionalità che l'Amministrazione Comunale di Pavia mette a disposizione dei suoi utenti al fine di usufruire dei servizi di rete ed in particolar modo dei servizi di tipo Internet/posta elettronica, devono essere utilizzati nel pieno rispetto delle norme del presente documento al fine di evitare possibili danni erariali, finanziari e di immagine all'Ente stesso.
2. Tutto il personale interessato dalle disposizioni del presente documento, è tenuto a contattare il responsabile della sicurezza informatica (leggasi Responsabile del Servizio Informatico Comunale o un suo delegato) prima di intraprendere qualsiasi attività non esplicitamente compresa nelle

disposizioni che seguono, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente.

Art. 4 Competenze e responsabilità

1. Le competenze e le responsabilità del personale dell'Amministrazione Comunale, per ciò che concerne l'utilizzo dei servizi di rete, sono definite nei commi seguenti e riassunti nello schema B allegato al presente documento.
2. Il Responsabile del Servizio Informatico Comunale è tenuto, anche avvalendosi di collaboratori, a:
 - a) informare tutti gli utenti sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'Ente;
 - b) assicurare che il personale a lui assegnato uniformi le proprie attività alle regole ed alle procedure descritte nel presente documento;
 - c) assicurare che i fornitori e/o eventuale personale incaricato esterno si uniformi alle regole ed alle procedure descritte nel presente documento;
 - d) elaborare delle regole per un utilizzo ragionevolmente sicuro del sistema informativo;
 - e) implementare delle policy di sicurezza sul *Sistema Informativo del Comune di Pavia*;
 - f) monitorare i sistemi per individuare un eventuale uso scorretto degli stessi, nel rispetto della privacy degli utenti;
 - g) predisporre del materiale informativo e divulgativo in materia di sicurezza informatica.
3. I dirigenti dei vari Settori sono tenuti a:
 - a) informare il personale sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'Ente;
 - b) assicurare che il personale si uniformi alle regole ed alle procedure descritte nel presente documento;
 - c) adempiere a tutti gli obblighi inerenti la titolarità loro affidata in materia di trattamento di dati personali gestiti dall'Amministrazione Comunale, come previsto dal Documento Programmatico sulla Sicurezza.
4. Il personale Comunale è responsabile per ciò che concerne:
 - a) il rispetto delle regole dell'Amministrazione per l'uso consentito del sistema informativo;
 - b) la segnalazione, senza ritardo, di ogni eventuale attività non autorizzata di cui sia venuto a conoscenza per motivi di ufficio;
 - c) ogni uso che venga fatto delle credenziali (account, passwords, user Id) assegnategli.

Art. 5 Titolarità

1. L'Amministrazione Comunale è titolare di tutte le risorse informative dell'Ente. Il personale dipendente e/o assimilato dovrà essere informato su quali siano gli usi consentiti e proibiti di tali risorse.
2. Ogni infrazione alle regole dell'Ente per un uso corretto del *Sistema Informativo del Comune di Pavia* costituirà una violazione della sicurezza ed esporrà l'utente ai provvedimenti previsti in tali casi, così come descritto all'articolo 22 del presente documento.

Capo 2 – Gli strumenti informatici

Art. 6 Acquisto di hardware e software

1. Per prevenire l'introduzione di virus e/o altri programmi dannosi e per proteggere l'integrità del *Sistema Informativo del Comune di Pavia*, tutto l'hardware ed il software in dotazione agli uffici deve essere assegnato dal Servizio Informatico Comunale, in quanto competente per la materia.
2. In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune aree, deve essere comunque richiesta per iscritto l'autorizzazione preventiva al Responsabile del Servizio Informatico Comunale, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti.

Art. 7 Rispetto della proprietà intellettuale e delle licenze

1. Tutto il software in uso nel *Sistema Informativo del Comune di Pavia* deve essere ottenuto seguendo le procedure e le linee guida dell'Ente e deve essere registrato a nome dell'Amministrazione Comunale. Tutto il personale è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright) e non può installare, duplicare o utilizzare qualsiasi tipologia di software al di fuori di quanto consentito dagli accordi di licenza.

Art. 8 Utilizzo di hardware o software di proprietà personale

1. Al fine di proteggere l'integrità del *Sistema Informativo del Comune di Pavia*, il personale non può utilizzare eventuale hardware o software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

Art. 9 Utilizzo delle apparecchiature elettroniche

1. L'utente è responsabile di ogni strumento di lavoro che utilizza e deve custodirlo con diligenza.
2. Le apparecchiature elettroniche (Personal Computer, Notebook, telefoni, smartphone, stampanti, scanner ecc.) in uso agli utenti sono considerate uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
3. Le apparecchiature elettroniche (Personal Computer, Notebook, telefoni, smartphone, stampanti, scanner ecc.) sono assegnate agli Uffici, Servizi e Settori e il consegnatario del bene è il dirigente

responsabile del Settore. In caso di cambio di mansioni dell'utente utilizzatore del bene, la strumentazione elettronica rimane nell'ufficio di assegnazione e di norma NON segue l'utente.

4. L'accesso all'elaboratore (PC, Notebook telefono mobile o smartphone) è protetto da password o da PIN che devono essere gestiti secondo quanto stabilito dal successivo art. 14.
5. Il Responsabile del Servizio Informatico Comunale e lo staff da lui diretto, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, previo consenso anche verbale dell'interessato;
6. Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile del Servizio Informatico Comunale o di un suo delegato ed una richiesta scritta da parte del dirigente responsabile dell'unità cui è assegnato il PC nella quale si dichiara che è stata rispettata la legge sul copyright (vedi modello C Allegato);
7. Il Personal Computer deve essere spento o bloccato (premendo i tasti Ctrl Alt Canc e poi Blocca Computer) ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
8. L'installazione e l'uso di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pen-drive, internet key, pc portatili ed apparati in genere ...), possono costituire una minaccia per la sicurezza dell'intero Sistema Informativo Comunale. Il loro utilizzo deve pertanto essere espressamente autorizzato dal Responsabile del Servizio Informatico Comunale o da un suo delegato che effettuerà di volta in volta una valutazione dei rischi connessi. La richiesta scritta per l'utilizzo di questi dispositivi deve essere effettuata da parte del dirigente o del responsabile dell'unità cui è assegnato il PC o l'utente (vedi modello C Allegato);
9. Non è consentita la redazione, la diffusione e 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.

Art. 10 Utilizzo dei supporti magnetici

1. Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce, Pen Drive, Cd o DVD riscrivibili) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione;
2. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave;
3. Non è consentito scaricare files contenuti in supporti magnetici/ ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
4. Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati / installati / testati. Nel caso di effettiva necessità di impiego devono essere

sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte del Responsabile del Servizio Informatico Comunale o di un suo delegato.

Art. 11 Utilizzo di dispositivi portatili e dei supporti per le presentazioni

1. Un dispositivo portatile, proprio per la sua natura deve essere oggetto di particolari attenzioni ed in particolare la sua custodia deve avvenire con diligenza oltre che durante l'utilizzo nel luogo di lavoro anche durante gli spostamenti.
2. Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, prestando particolare attenzione, per i portatili dati in "prestito", alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
3. Tutti coloro che utilizzano i supporti per le presentazioni, salvo diversi ed espliciti accordi, sono tenuti a ritirarli presso il Servizio Informatico Comunale e a riconsegnarli di norma entro 1 ora dal termine dell'evento. Qualora l'evento termini al di fuori dell'orario lavorativo, la strumentazione dovrà essere consegnata al Servizio Informatico Comunale il primo giorno lavorativo utile.
4. I PC portatili e tutti gli altri supporti per le presentazioni utilizzati all'esterno (convegni etc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.
5. Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o verso internet, devono essere autorizzate esclusivamente a cura del Responsabile del Servizio Informatico Comunale o di un suo delegato. E' vietato utilizzare le suddette connessioni (comprese le chiavette per l'accesso alla rete Internet e connessioni Wi-Fi all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN).

Art. 12 Protezione dai virus

1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o ogni altro software aggressivo.
2. Ogni utente è tenuto a controllare la presenza ed il regolare funzionamento e l'aggiornamento periodico del software antivirus installato (presenza dell'icona ,).
3. Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
 - a) sospendere ogni elaborazione in corso **senza spegnere il computer;**
 - b) segnalare l'accaduto al Servizio Informatico Comunale.

Capo 3 - La rete aziendale e Internet

Art. 13 Utilizzo della rete del Comune di Pavia

1. Le unità di rete e le cartelle condivise sui server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, verranno svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema.
2. Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto di replicare su dischi locali dei PC dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione del Responsabile del Servizio Informatico Comunale o di un suo delegato e senza l'adozione di adeguate politiche di sicurezza, quali la crittazione dei dati stessi e l'adozione di politiche di backup comprensive della dotazione di idonei archivi protetti.
3. E' assolutamente proibito entrare nella rete e nei programmi con nomi utente diversi dai propri o dal proprio nel caso di accesso univoco.(Global Sign-On).
4. Il Responsabile del Servizio Informatico Comunale tramite il proprio staff, può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza, oppure non attinente all'attività lavorativa a fronte di controlli a campione sia sui PC degli incaricati sia sulle unità di rete.
5. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.
6. E' cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
7. Al fine di consentire il salvataggio in totale sicurezza e riservatezza dei propri dati locali e personali (compresi i messaggi di posta elettronica) vengono messe a disposizione sui server dell'Ente delle idonee cartelle. In particolare, ogni utente ha mappato un disco virtuale chiamato **W:** che punta ad un server sul quale può essere effettuato backup dei propri dati. Lo spazio disponibile è ad accesso esclusivo dell'utente stesso, ma in ogni caso ciò non implica che tale spazio possa essere utilizzato per fini NON LAVORATIVI.

Art. 14 Gestione delle Password

1. Per le password gli utenti devono adottare i seguenti criteri:
 - lunghezza non inferiore a 8 caratteri;
 - non deve contenere nomi comuni;
 - non deve contenere nomi di persona;
 - deve essere diversa dallo User-ID.
 - deve essere diversa dalle precedenti password
2. In modo particolare per alcuni applicativi gestionali si è riscontrato che le password utilizzate NON rispecchiano i criteri di sicurezza sopra enunciati, pertanto entro 30 giorni dall'approvazione di

questo documento, tutti gli utenti dell'applicazione saranno tenuti a cambiare la propria password con una che abbia le caratteristiche sopra descritte.

3. Viene ricordato, inoltre, agli utenti che la password è riservata e personale, non deve essere comunicata a nessuno, deve essere memorizzata e non deve essere trascritta.
4. Qualora ragioni organizzative rendessero necessario l'accesso alla rete o ad un PC con le credenziali di un altro utente, il dirigente o il responsabile del Servizio dovranno richiedere in forma scritta (anche via e-mail) all'Amministratore di Sistema l'emissione di una nuova password
5. Le password utilizzate dagli incaricati al trattamento, salvo diversi obblighi o disposizioni, hanno una durata massima di **6 mesi**, trascorsi i quali le password devono essere sostituite.
6. La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.
7. I dirigenti comunicheranno tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia al Servizio Amministrazione ed Organizzazione delle Risorse Umane che al Servizio Informatico Comunale, per iscritto, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario (vedi modello C Allegato).

Art. 15 Uso della rete Internet e dei relativi servizi

1. Gli utenti sono tenuti ad utilizzare il collegamento ad Internet unicamente per motivi legati ai propri doveri di ufficio. Sono pertanto vietati a titolo esemplificativo:
 - l'uso di Internet per lo scarico di file soggetti a copyright non legati ad un uso d'ufficio;
 - l'uso e la navigazione su siti non legati ad esigenze esclusivamente di tipo lavorativo. A tal fine l'amministratore del firewall provvederà ad inibire la consultazione dei siti web non utili alla produttività dell'Ente e, soprattutto, potenzialmente lesivi per l'infrastruttura;
 - l'utilizzo di qualsiasi mezzo alternativo (modem, reti wireless, Internet Key o altro) al collegamento Lan dell'Ente per connettersi ad Internet se non espressamente autorizzato;
 - lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e di internet in qualsiasi modo;
 - lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile del Servizio Informatico Comunale o da un suo delegato;
 - l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dall'Ente o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto;
 - ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;

- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta.
2. Il Servizio Informatico Comunale si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione e con i Dirigenti, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
 3. Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.
 4. È buona norma che ogni utente esegua una periodica manutenzione del proprio browser anche attraverso la pulizia dei cookies e dei files temporanei di internet. Il SIC è disponibile a fornire il supporto necessario per tale scopo.

Capo 4 - La posta elettronica

Art. 16 Principi generali

1. La posta elettronica è uno dei mezzi di comunicazione e di trasmissione di documenti, informazioni e dati dell'Ente.
2. Il servizio di posta elettronica è destinato al conseguimento dei fini istituzionali dell'Ente.
3. Il servizio di posta elettronica è operante con continuità 24 ore al giorno per 365 giorni l'anno.
4. Il Comune fornisce a tutti i propri dipendenti, al Sindaco, al Vice Sindaco, agli Assessori, al Presidente del Consiglio e ai Consiglieri una casella di posta elettronica personale che può essere certificata o non (casella personale).
5. Il Comune fornisce a tutti i propri uffici interni una casella di posta elettronica (casella di struttura).
6. Il Comune può fornire una casella di posta elettronica ai propri collaboratori, previa richiesta del Dirigente della struttura di afferenza (vedi modello C Allegato).
7. Gli utenti hanno l'obbligo di procedere alla tempestiva lettura della corrispondenza pervenuta nella propria casella, almeno una volta al giorno quando sono in servizio.
8. La posta elettronica certificata è una particolare posta elettronica in grado di garantire in modo certo l'identità del mittente e la consegna del messaggio. La casella di posta elettronica istituzionale dell'Ente registrata all'IPA (Indice delle Pubbliche Amministrazioni) è: protocollo@pec.comune.pavia.it. Questa casella è collegata in modo diretto con il software di

protocollo dell'Ente attraverso il quale è possibile ricevere e spedire messaggi di posta con validità legale e certezza di recapito.

9. Si rammenta che la certificazione di ricezione e/o consegna di un messaggio di posta elettronica ha validità legale solo se la comunicazione avviene fra 2 caselle certificate. Si sottolinea altresì che la PEC garantisce il canale di comunicazione ma non il contenuto del messaggio che per avere piena validità dovrà essere firmato digitalmente.
10. L'apertura di una nuova casella PEC deve essere espressamente autorizzata dal Responsabile del Servizio Informatico Comunale, previa richiesta del Dirigente della struttura di appartenenza (vedi modello C Allegato).

Art. 17 Gestione del servizio

1. Il servizio di posta elettronica è gestito dal Servizio Informatico Comunale, cui è assegnata la responsabilità del suo corretto funzionamento. In particolare, il Servizio Informatico Comunale è tenuto a:
 - adottare le misure più idonee a garantire la continuità, la disponibilità e la sicurezza del servizio;
 - gestire i dati degli utenti nel rispetto della vigente normativa sulla tutela dei dati personali;
 - informare tempestivamente gli utenti, con un anticipo almeno di 24 ore, di eventuali interruzioni del servizio che si rendessero necessarie per cause di forza maggiore;
 - monitorare i livelli di servizio del sistema al fine di garantirne la massima efficienza;
 - monitorare l'utilizzo del servizio da parte degli utenti anche attraverso eventuali controlli a campione, al fine di evidenziarne usi scorretti o non consentiti;
 - offrire assistenza tecnica agli utenti.
2. Il Servizio Informatico Comunale non effettua alcuna visura, controllo, censura, modifica, cancellazione dei messaggi di posta elettronica ricevuti e inviati dagli utenti, a meno che ciò non venga richiesto dalla legge ovvero nel caso in cui ciò si renda necessario per adempiere ad una disposizione di legge, ad un ordine giudiziario o governativo.
3. Al fine di prevenire e ridurre per quanto possibile la ricezione di Spam (e-mail spazzatura), è attivo un sistema di antispam che automaticamente elimina messaggi ritenuti "spazzatura" in base a particolari algoritmi e black list. L'affinamento del software è continuo ma è possibile che ci siano dei "falsi positivi" (e-mail eliminate erroneamente dal software antispam) o dei "falsi negativi" (e-mail che superano il controllo antispam ma che in realtà sono spazzatura). Ogni segnalazione di malfunzionamento dell'algoritmo è ritenuta preziosa per l'evoluzione del sistema.

Art. 18 Gestione delle caselle di posta elettronica

1. Il Servizio Informatico Comunale provvede ad attivare automaticamente per ogni dipendente, conseguentemente alla sua assunzione in servizio (se opportunamente comunicata), una casella di posta elettronica personale.

2. Il Servizio Informatico Comunale provvede a disattivare automaticamente per ogni dipendente, conseguentemente alla sua cessazione dal servizio, la relativa casella di posta elettronica personale.
3. Al fine degli adempimenti di cui sopra, l'UOI Stipendi e/o il Servizio Amministrazione ed Organizzazione delle Risorse Umane provvederanno mensilmente a comunicare al Servizio Informatico Comunale l'elenco del personale assunto/cessato nel mese precedente.
4. Il Servizio Informatico Comunale provvede ad attivare/disattivare caselle di posta elettronica per gli Organi Politici dell'Ente.
5. Il Servizio Informatico Comunale provvede ad attivare/disattivare caselle di posta elettronica per i collaboratori, previa richiesta scritta del Dirigente della struttura di appartenenza effettuata con apposito modulo (vedi modello C Allegato).
6. L'attivazione di una casella di posta elettronica è effettuata attraverso l'assegnazione di un codice identificativo dell'utente (userid), la relativa parola chiave riservata (password) iniziale ed un indirizzo.
7. Gli indirizzi di posta elettronica per le caselle personali hanno la seguente nomenclatura, salvo casi di omonimia od esigenze particolari:
 <nome utente>.<cognome utente>@comune.pv.it
8. Gli indirizzi di posta elettronica per le caselle degli uffici hanno la seguente nomenclatura, salvo casi particolari:
 <nome, abbreviazione o acronimo della struttura>@comune.pv.it
9. Sarà cura del Servizio Informatico Comunale uniformare a questo standard tutte le caselle di posta entro 6 mesi dall'approvazione del presente documento. Per garantire la "retrocompatibilità" verrà mantenuta attiva anche la "vecchia" notazione per un periodo di 2 anni dall'approvazione del presente documento.

Art. 19 Compiti e responsabilità

1. Il dipendente e/o collaboratore è responsabile della casella di posta elettronica assegnatagli, del contenuto dei messaggi inviati e di tutte le operazioni effettuate con la casella di posta elettronica relativa allo userid a lui associato.
2. L'utente è responsabile delle eventuali conseguenze pregiudizievoli che un uso improprio del servizio da parte del proprio userid potrebbero comportare a terze persone, e ciò in riferimento alla vigente normativa in materia civile e penale.
3. Il Dirigente, o responsabile di servizio, è parimenti responsabile della casella di posta elettronica dell'ufficio che dirige.
4. Il Dirigente, o responsabile di servizio, può delegare uno o più dipendenti alla gestione della casella dell'ufficio. La delega va attribuita per iscritto.

5. È buona norma che ogni assegnatario di casella di posta elettronica esegua una manutenzione di base della stessa, che preveda la suddivisione dei messaggi in sottocartelle al fine di evitare la possibile perdita dei messaggi stessi. Il SIC è disponibile a fornire il supporto necessario per tale scopo.

Art. 20 Utilizzazione del servizio

1. L'utente è tenuto ad attenersi alle seguenti prescrizioni nell'utilizzo del servizio di posta elettronica:
- conformarsi alle indicazioni tecniche fornite dal Servizio Informatico Comunale;
 - non utilizzare la posta elettronica per trasmettere e diffondere materiali che non possono essere legalmente distribuiti per via telematica;
 - non usare il servizio per scopi illegali, per inviare o ricevere materiale pornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso;
 - non inviare e ricevere materiali e/o messaggi che incoraggino terzi a mettere in atto una condotta illecita e/o criminosa passibile di responsabilità penale o civile;
 - non utilizzare il servizio per inviare catene di lettere, solleciti commerciali, messaggi politici ovvero qualunque altro messaggio a persone che non abbiano acconsentito a tale procedura;
 - non utilizzare il servizio per motivi privati e/o per contatti interpersonali tra i dipendenti non inerenti l'uso d'ufficio;
 - non inviare messaggi ad una pluralità di destinatari (invii multipli) indiscriminatamente, eccedenti il numero dei reali interessati;
 - utilizzare con diligenza il servizio, evitando di sovraccaricare il sistema con l'invio di messaggi ed allegati di dimensioni inutilmente eccessive e/o contenenti inutili grafismi od immagini (la dimensione massima degli allegati concessi è di 5 Mb);
 - cancellare messaggi ricevuti inutili e di dimensioni eccessive;
 - utilizzare il servizio nel pieno rispetto del Codice di tutela dei dati personali.

Art. 21 Pubblicità degli indirizzi

1. Il Servizio Informatico Comunale ha cura della gestione, aggiornamento e pubblicazione dell'elenco degli indirizzi di posta elettronica. Tale elenco è reso disponibile per la consultazione, sia all'interno che all'esterno dell'Ente, mediante pubblicazione degli stessi sul sito Internet Comunale.

Capo 5 – Disposizioni finali

Art. 22 Violazioni

1. Qualsiasi utilizzo non conforme alle disposizioni del presenti Linee e/o alle leggi vigenti è ad esclusiva responsabilità dell'utente.

2. L'Amministrazione Comunale si riserva la facoltà di verificare, nel pieno rispetto della normativa vigente in tema di privacy, l'attuazione delle disposizioni del presente documento attraverso la periodica consultazione di statistiche anonime sull'uso di internet, posta elettronica e delle strumentazioni di lavoro.
3. Qualora venissero riscontrate diffuse anomalie, il controllo potrà essere progressivamente ristretto per individuare con più precisione "l'area" fisica od organizzativa dalla quale provengono tali utilizzi anomali.
4. Nei casi di accertata violazione di tali norme, è demandata ai rispettivi Dirigenti l'applicazione dei necessari provvedimenti disciplinari nei confronti dei responsabili, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituenti reato.

Art. 23 Aggiornamento e revisione

1. Il presente Documento è soggetto a revisione con frequenza annuale, contestualmente all'approvazione del Documento Programmatico sulla Sicurezza, così da diventarne parte integrante.

Art. 24 Disposizioni finali

1. Per quanto non disciplinato dal presente Documento, si rimanda alla legislazione vigente in materia, con particolare riguardo alla Deliberazione - 01 marzo 2007 del Garante per la Privacy Bollettino del n. 81/marzo 2007 che si allega per completezza (Allegato D).

Allegato A GLOSSARIO DEI TERMINI TECNICI E/O INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una userId e di una password, consente l'accesso alla rete e/o ai servizi. Ad esempio, un account (ottenuto con un abbonamento ad un ISP) ci permette di entrare in Internet, un altro account (spesso con un altro server, gratuito) ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti. Altri account servono per accedere a server e servizi quali enciclopedie, notiziari, shareware...
Antivirus	Tipo di software che cerca e distrugge gli eventuali programmi virus e cerca di rimediare ai danni che hanno compiuto.
Attachment/Allegato di posta elettronica	File o Documento di qualunque genere agganciato ad un messaggio di posta elettronica per essere inviato a distanza.
AVI (Audio Video Interleaved)	Formato per file video. I dati del video e dell'audio sono memorizzati in pacchetti alternati. I video AVI hanno un'ottima qualità di riproduzione, ma i suoi file sono molto più grossi degli altri formati video.
Backup	Copia di riserva di un disco, di una parte del disco o di uno o più file.
Browser	Software che consente la visualizzazione della pagine di Internet e/o Intranet. Spesso deve essere affiancato da plug-in per rendere attive determinate funzionalità come il suono ed i filmati. I due browser più importanti sono Netscape Navigator e Microsoft Internet Explorer. Ne esistono altri minori, quali Mosaic e Opera. Può essere utilizzato anche per la consultazione di pagine HTML in locale.
Chat (webchat)	Sistema che consente il dialogo (tramite digitazione sulla tastiera) di più utenti contemporaneamente tramite Internet. I chat possono essere pubblici (ognuno legge i messaggi di tutti gli altri ed invia i propri a tutti i presenti) o privati (ospitati in "stanze" virtuali).

Client	Personal collegato ad un server tramite rete locale o geografica, ed al quale richiede uno o più servizi. Alcuni software, come i database, sono divisi in una parte client (residente ed in esecuzione sul personal per la consultazione o la modifica del database) ed una parte server (residente ed in esecuzione sul server per gestire il database e rispondere alle interrogazioni dei client).
Client di posta elettronica	Software che, collegandosi ad un server, consente lo scambio di messaggi e di file attraverso il servizio di posta elettronica. Il client standard all'interno del S.I.P. è attualmente Microsoft Outlook.
Crittografia	Invio di dati resi incomprensibili e che è possibile decodificare solamente tramite apposito hardware e/o software. Esistono diversi tipi di crittografia e la decodifica dipende, comunque, da una parola chiave o da una smart card. Il metodo più utilizzato è quello a chiave pubblica.
Database	(Base di Dati) Qualsiasi aggregato di dati organizzato in campi (colonne) e record (righe).
Download	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).
E-mail	Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede a inoltrarli al destinatario quando questo si collega.
Firewall	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.

Freeware	Software realizzato e distribuito da privati o piccole società, attraverso Internet od i CD-ROM allegati alle pubblicazioni in edicola. Il programma è pienamente funzionante e non è necessario pagare nulla, anche se a volte si tratta di software molto utile. A volte l'autore chiede l'invio di una cartolina di ringraziamento (cardware), altre volte un versamento per beneficenza ad ospedali od altri organismi.
Hardware	letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, HARD DISK, ecc.) che costituiscono un computer.
HTML	Linguaggio di programmazione utilizzato in Internet e pubblicato nel 1991. Serve a creare documenti di testo e grafica che siano visualizzabili da qualsiasi sistema, tramite comandi incorporati nel documento stesso. Rispetto ai precedenti GML e SGML, ha dei comandi che rendono 'attive' parti del testo o della grafica: cliccando su uno di questi punti, il link, viene richiamato sullo schermo un altro documento. Il documento, quando viene visualizzato, viene chiamato pagina. Una pagina, se divisa in frame, può essere composta da più di un documento, uno per ciascuna frame. Per visualizzare le pagine Internet è necessario un software apposito chiamato browser, e visualizzare una serie di pagine viene chiamato navigare. Un gruppo di pagine registrate sullo stesso server ed aventi, in genere, lo stesso argomento, si chiama sito.
Internet	La madre di tutte le reti di computer. È l'insieme mondiale delle reti di computer interconnesse mediante il protocollo TCP/IP
Intranet	Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.
Lan (Local Area Network)	Una rete che collega computer e periferiche (es. stampanti, fax, scanner...) installate nella stessa sede (es. stesso palazzo, anche a piani diversi) oppure in sedi vicine (es. due palazzi adiacenti) in modo che non serva ricorrere a servizi di trasmissione dati esterni, cittadini, regionali, nazionali ed internazionali.
Mailing list	Lista di distribuzione automatica di messaggi di posta elettronica, riguardanti un determinato argomento. I messaggi sono inviati ad un list server, che li archivia e provvede ad inviarli automaticamente agli iscritti.

Modem (modulatore/demodulatore) Apparecchiatura che consente di inviare e ricevere i dati digitali del computer tramite le linee analogiche del telefono oppure le linee digitali ISDN.

MP3 ((MPEG-4 Audio Layer III) Tecnologia, emessa nel 1998 dal comitato MPEG, per la compressione/decompressione di file audio che consente di mantenere una perfetta fedeltà e qualità anche riducendo il file audio (ripreso da un Cd audio) di ben 11 volte la lunghezza originale. Un file che contiene 5 minuti di musica stereo (in due canali da 16 bit a 44.100 MHz) passa dai 60 Mb del file originale, ai soli 5 Mb del file MP3, pur mantenendo la stessa qualità che si otterrebbe da un CD audio. La compressione può variare da un minimo di 5 volte (con un brano da CD audio a 32 Kb al secondo) ad un massimo di 176 volte (audio solo vocale, senza musica a 1 Kb al secondo). L'MP3 ha infatti fatto sviluppare la pirateria musicale sul fronte di Internet: un file MP3 viene trasferito dal server al computer in circa 20 minuti. Da molti siti è possibile scaricare file audio di canzoni, anche le più recenti; dotandosi di un masterizzatore CD (compatibile con i CD audio) è possibile riprodurre un CD audio pirata perfetto, oppure prepararsi un CD personalizzato con canzoni di cantanti diversi. Alla base del MP3 c'è il Layer III, elaborato dal IIS

MPG (Motion Picture Experts Group) Comitato formato nel 1988 da membri ISO e IEC che stabilisce gli standard digitali per audio e video. Ha emesso gli standard JPEG e MPEG. Ricordiamo, tra gli altri:

MPEG-1

Standard, emesso nel 1993 dal comitato MPEG, per la registrazione di file audio e video su VideoCD con qualità simile ai nastri VHS e risoluzione di 360x288 pixel ed un bit rate costante di 1,5 Mbit al secondo. Contrassegnato dalla sigla ISO 11172.

MPEG-2

Evoluzione del formato MPEG-1, che consente una risoluzione di 720x576 pixel in PAL (25 quadri al secondo) o di 720x480 in SECAM (30 quadri al secondo) ed un bit rate più elevato, quindi una riproduzione dell'immagine molto migliore. Lo standard MPEG-2 è stato adottato dalla televisione digitale, terrestre e via satellite, e dai produttori di DVD in quanto riesce a combinare velocità e qualità

Password

Parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito Internet. E' necessario digitarla esattamente, assieme alla user-id. Alcuni software distinguono fra lettere maiuscole e minuscole. E' consigliabile non scriverla su bigliettini od agende, né utilizzare parole troppo semplici da indovinare (es: il proprio nome, il numero di telefono o la data di nascita). Se l'accesso è ad alta protezione, la password deve avere un numero minimo di caratteri, deve essere alfanumerica, e può essere previsto un intervallo regolare per la sua modifica (es: ogni mese). Occorre anche fare attenzione alle finestre di dialogo che richiedono la password: spesso è possibile istruire il programma od il sistema a ricordare ed immettere automaticamente la password, ma allora chiunque si collega con lo stesso computer ha libero accesso.

Plug-in

Software accessorio che aggiunge determinate funzioni ai programmi, ad esempio ai programmi di grafica od ai browser. Nei programmi di grafica i plug-in possono consentire l'uso di determinate periferiche, oppure l'esecuzione sull'immagine di effetti e di elaborazioni, di applicazioni di filtri. Ad un browser consentono funzioni come la visualizzazione di video, il collegamento con telecamere in diretta, l'ascolto di musica, il dialogo a voce fra più utenti, ed altro durante la visualizzazione delle pagine Internet.

Policy

Insieme di regole che determina quali contenuti possano passare attraverso una rete. Ad esempio, in una accesso Internet, possono essere bloccati contenuti di tipi erotico, sessuale, commerciale, di gioco...

Quicktime

Standard definito dalla Apple e utilizzata da tutti i computer per la riproduzione fedele dei filmati video. E' previsto un plug-in QuickTime per i programmi di navigazione in Internet.

S.I.P.U.

Sistema Informativo della Provincia di Udine. E' l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Amministrazione Provinciale di Udine.

Server	Computer dedicato allo svolgimento di un servizio preciso, come la gestione di una rete locale o geografica, alla gestione delle periferiche di stampa (print server), allo scambio e condivisione di dati fra i computer (file server, database server), all'invio o inoltro di posta elettronica (mail server) od a contenere i file di un sito web (web server). Utilizza un sistema operativo di rete. I computer collegati e che utilizzano il servizio del server, si chiamano client. A volte lo stesso computer svolge diverse funzioni di server (es: sia file server che print server).
Shareware	Software realizzato e distribuito da privati o piccole società, attraverso Internet od i CD-ROM allegati alle pubblicazioni in edicola. L'utilizzatore può provare il programma prima di acquistarlo, nel caso basta inviare un messaggio di posta elettronica all'autore con i dati della propria carta di credito (o direttamente inviare i soldi via posta ordinaria) per ricevere un codice che, inserito nel programma, ne consente l'uso completo. Infatti certe funzionalità importanti, o i livelli finali nei giochi, sono spesso bloccati e disponibili sono dopo la registrazione dell'acquisto. Il costo, comunque, è molto inferiore a quello dei prodotti commerciali, anche se certi programmi shareware non hanno nulla da invidiare a quelli commerciali. Visto che il prezzo è molto basso (dai 10 ai 50 dollari), è sempre conveniente registrarsi e pagare, così si potranno ricevere gli aggiornamenti ed altri programmi dello stesso autore, nonché dare un contributo allo sviluppo di software a prezzo contenuto.
Software	sono i programmi (professionali, ludici, video, musicali, raccolte di suoni ed immagini) per i computer.
UserId	Nome utente
Utente (User)	Chiunque utilizzi un elaboratore collegato alla rete del SIPU, sia che il collegamento avvenga in rete locale, come avviene all'interno delle sedi provinciali, sia che si tratti di un accesso remoto, come avviene nei collegamenti via modem.
Virus	Un programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.

Allegato B Responsabilità per l'uso consentito del S.I.C.

Attività	Responsabile S.I.C.	Dirigenti	Tutto il personale
Informazione agli utenti	X	X	
Erogazione sanzioni disciplinari		X	
Acquisto hardware-software in modo appropriato	X		
Rispetto delle norme sul diritto d'autore, diritti di licenza	X	X	X
Rispetto delle norme sul software di proprietà personale	X	X	X
Rispetto della proprietà intellettuale	X	X	X
Rispetto delle norme sull'uso della e-mail	X	X	X
Rispetto delle norme sull'utilizzo di Internet	X	X	X
Rispetto delle norme sull'utilizzo del sistema info. Prov.	X	X	X

X = responsabile per il rispetto delle norme



COMUNE DI PAVIA

AL SERVIZIO INFORMATICO COMUNALE

SEDE

OGGETTO: richiesta al Servizio Informatico Comunale

Il sottoscritto _____

Responsabile del Settore / Servizio/ Ufficio _____

CHIEDE

1. l'autorizzazione all'installazione del seguente software: _____
_____ sui
seguenti P.C.: _____

precisando che è stata rispettata la legge sul copyright:

2. l'autorizzazione all'installazione sul PC _____ o
un I.AN del seguente dispositivo: _____

3. l'apertura/chiusura (cancellare la voce non idonea) della casella di posta elettronica per il
proprio collaboratore: _____

l'apertura/chiusura (cancellare la voce non idonea) della casella di posta elettronica denominata:

_____ che dovrà essere

gestita dalle seguenti persone: _____

l'apertura/chiusura (cancellare la voce non idonea) della casella di posta elettronica certificata

(PEC) denominata: _____

oppure **COMUNICA**

che il dipendente _____ ha

cambiato mansione e che pertanto gli devono essere revocati tutti i precedenti diritti di accesso

alle risorse di rete ad assegnati ex-novo i seguenti: _____

legati al suo nuovo ruolo che risulta essere: _____

che il dipendente _____ ha

cambiato mansione e che pertanto ai precedenti diritti di accesso alle risorse di rete devono

essere aggiunti i seguenti: _____

legati al suo nuovo ruolo che risulta essere: _____

Pavia,

Firma del Responsabile richiedente _____



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.

1.2. 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.

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).

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*).

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. S. 4001, 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 videotermini", il quale esclude la possibilità del controllo informatico "all'insaputa dei lavoratori"*).

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 constatati 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 (*cf. 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.

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. È 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. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (*art. 11, comma 2, del Codice*).

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. Ciò, anche in presenza di attività di controllo di continue.

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, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

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 le tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet;
- 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 *file* che prevenivano 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 - cioè non 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).

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, ufficio reclami@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;
- 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. 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 (concesso 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 sui 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; Regolamento 2001/2001 art. 12, 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 prevenivano 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 o 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 6.1.1)

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), *siccome 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

Letto, approvato e sottoscritto.

IL PRESIDENTE

f.to SINDACO ALESSANDRO CATTANEO

IL SEGRETARIO GENERALE

f.to DOTT. PIETRO PAOLO MILETI

DICHIARAZIONE DI PUBBLICAZIONE

Si certifica che ai sensi dell'art. 124 del d.lgs n.267 del 18/8/2000 copia della deliberazione sopra estesa viene pubblicata all'Albo Pretorio on line disciplinato dall'art. 32, comma 1, della L. 69/2009

dal 23 DICEMBRE 2011	al 6 GENNAIO 2012
Addi, 22 DICEMBRE 2011	

IL SEGRETARIO GENERALE

f.to DOTT. PIETRO PAOLO MILETI

Comunicata ai Capi Gruppo Consiliari con elenco n. 78 il 23 DICEMBRE 2011

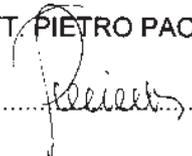
Divenuta esecutiva il per decorrenza dei termini di cui all'art. 134, comma 3, del D.Lgs. n. 267 del 18/8/2000.

IL SEGRETARIO GENERALE

Copia conforme all'originale per uso amministrativo.

Addi 22 DICEMBRE 2011

IL SEGRETARIO GENERALE
DOTT. PIETRO PAOLO MILETI


.....