Città di **Pioltello**

DOCUMENTO AZIENDALE SULLA SICUREZZA ED IL TRATTAMENTO DATI

versione 3.3 - 21 novembre 2015

Il Dirigente del Settore Affari Generali

PREMESSO CHE

- ai sensi e per gli effetti dell'art. 34, comma 1, lettera g), del D.Lgs. 196/2003, e del disciplinare tecnico allegato al decreto medesimo era fatto obbligo di adottare il documento programmatico sulla sicurezza (DPS) contenente le linee guida in base alle quali l'Ente pianifica e gestisce con opportuni standard la sicurezza della rete informatica;
- il titolare del trattamento dei dati per il Comune di Pioltello è individuato nel rappresentante legale dell'Ente, la sede del trattamento dei dati è presso la sede centrale del Comune di Pioltello, Via C. Cattaneo, 1, CAP 20096, c.f. 83501410159 - p.i. 00870010154, nonché nelle ulteriori sedi e sportelli presenti sul territorio comunale;
- il Titolare del trattamento, come sopra individuato, ha nominato con proprio provvedimento diversi Responsabili del trattamento dei dati;
- la Giunta Comunale, giusto quanto disposto dall'art. 61, comma 1 del D.P.R. 445/2000, con propria deliberazione n.242 del 22 dicembre 2003 ha individuato come Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi il Dirigente pro-tempore del Settore Affari Generali il quale riveste anche il ruolo di dirigente dell'U.O. Informatica dell'ente;
- pur essendo venuto meno l'obbligo formale di redazione del DPS, è comunque acclarato che fra gli obblighi del dirigente responsabile delle gestione del flusso documentale e dei sistemi informatici vi sia la definizione di norme per la sicurezza e il trattamento dei dati;
- al fine tutelare l'Ente si ritiene opportuno elaborare un documento che riassuma le prescrizioni adottate e da adottarsi in materia di sicurezza e trattamento dei dati anche in considerazione del fatto che, allo stato attuale, sono in corso interventi in materia di revisione del sistema di protocollo e gestione del flusso documentale e in materia di informatizzazione delle procedure;

APPROVA

nel seguente testo il

DOCUMENTO AZIENDALE SULLA SICUREZZA ED IL TRATTAMENTO DATI.

Il documento verrà pubblicato sul portale dell'ente, nell'area intranet e sarà punto di riferimento per la formazione del personale in materia.

Pioltello 23 NOV 2015

COMUNE DI PIOLTELLO Prov. di Milano

Il Dirigente del Settore Affari Generali
(Dott. Andrea Novaga)

Art. 1. Elenco dei trattamenti di dati attuati dall’Ente

L’Ente effettua il trattamento dei dati esclusivamente per le finalità necessarie al perseguimento dei fini istituzionali nonché a quelle connesse e correlate.

Ogni struttura tratta i dati pertinenti con le finalità istituzionali dell’Ente, anche di concerto con altre strutture dell’Ente medesimo.

Il trattamento di dati sensibili e giudiziari viene effettuato con le finalità e per le operazioni previste giusto quanto disposto dall’art. 8 del Regolamento Comunale sul trattamento e la tutela dei dati personali e tabelle annesse, approvate dal Garante con proprio provvedimento generale.

Per quanto concerne il trattamento dei dati sensibili e giudiziari adotta le più severe misure di sicurezza richieste dalla vigente normativa ed effettua periodiche verifiche al fine di mantenere il più alto standard di sicurezza possibile per la più efficace tutela delle proprie banche dati.

Vengono effettuati periodici riallineamenti dei prodotti e delle misure adottate al fine di rendere il sistema il più aggiornato possibile in materia di riservatezza e protezione dei dati, e vengono attuate procedure di controllo, verifica e conformità avendo riguardo ai più recenti standard presenti e rilasciati.

Dall’Ente vengono trattati dati di natura giudiziaria per ottemperare a specifiche disposizioni di legge (elettorale, pubblica sicurezza, servizi sociali) che non formano una specifica, o specifiche banche dati, ma sono informazioni che rientrano in banche dati esistenti per l’attuazione di dette specifiche finalità.

Il Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, individuato dalla Giunta comunale nel Dirigente pro-tempore del Settore Affari Generali è la figura cui spetta promuovere lo sviluppo ed il mantenimento dei programmi di sicurezza contenuti nel presente documento; informa il Titolare del trattamento sulle eventuali non corrispondenze con le norme di sicurezza e sugli eventuali episodi di criticità che dovessero emergere; promuove ed organizza la somministrazione di un adeguato programma di addestramento degli incaricati al trattamento e mantiene attivo un adeguato programma di verifica, controllo e monitoraggio, così anche come disposto dalla vigente legislazione in materia.

Agli addetti del Servizio Informatico Comunale (nel seguito: "S.I.C.") spetta il compito di promuovere lo sviluppo ed il mantenimento dei programmi di sicurezza contenuti nel presente provvedimento nonché quello di segnalare al Responsabile, come sopra individuato, le eventuali necessità per mantenere il livello di sicurezza sempre il più possibile aggiornato alle regole della tecnica.

Sempre al S.I.C. spetta il compito di garantire il funzionamento di tutti i dispositivi elettronici, degli strumenti, dei sistemi operativi, dei software, con particolare riferimento ai sistemi antivirus, firewall, al sistema di backup, al sistema di ripristino dati, alle reti, al controllo degli accessi. Tali funzioni verranno erogate sia direttamente sia per mezzo di software-house e consulenti esterni.

Conformemente alle disposizioni del Garante del 27 novembre 2008, pubblicate in Gazzetta Ufficiale n. 300 del 24-12-2008 e i provvedimenti successivi, l'Ente ha predisposto e attuato un percorso per giungere alla corretta individuazione e gestione degli oneri posti a verifica dell'operatività degli amministratori di sistema adottando idonee misure anche di natura logico-informatica.

La struttura dell’Ente è suddivisa in Settori e Unità Organizzative.

Si ribadisce che i Responsabili sono individuati nei Dirigenti pro-tempore dei diversi settori nonché nel Comandante della Polizia Locale.

Per tutti i settori dell’Ente valgono le seguenti informazioni comuni.

I locali utilizzati per il trattamento dei dati si possono suddividere in un ufficio riservato a ciascun Dirigente e al Responsabile della Polizia Locale e uno o più locali, distinti dai precedenti, ove svolgono la loro opera diversi operatori che possono condividere gli spazi con il pubblico che viene ricevuto o ad appositi sportelli (ove esiste una separazione fisica con gli operatori e viene garantito il rispetto della riservatezza) o in appositi spazi (come nei servizi alla persona il cui l'utente è fatto accomodare in idonea stanza in cui può liberamente dialogare con l'addetto) sia in ambiente promiscuo ad accesso individuale su invito dell'operatore (come negli spazi dello Sportello del Cittadino).

Gli strumenti utilizzati per il trattamento dei dati possono essere elettronici o cartacei.

I trattamenti dei dati che vengono effettuati sono elencati nella tabella che segue.

codice	trattamento	tipo di dato C = comune S = sensibile G = giudiziario	strumenti utilizzati
1	Inserimento dei dati	C, S, G	personal computer, supporto cartaceo
2	Modifica dei dati	C, S, G	personal computer, supporto cartaceo
3	Cancellazione dei dati	C, S, G	personal computer, supporto cartaceo
4	Consultazione dei dati	C, S, G	personal computer, supporto cartaceo
5	Elaborazione dei dati	C, S, G	personal computer, supporto cartaceo
6	Stampa dei dati su carta e su file	C, S, G	personal computer, supporto cartaceo
7	Comunicazione a terzi (Enti ed organismi con i quali la struttura collabora per finalità istituzionali e/o in funzione di legge o di regolamento)	C, S, G	personal computer, supporto cartaceo
8	Distruzione dei dati	C	personal computer, supporto cartaceo
9	Manutenzione software procedure usate per il trattamento dei dati	C, S, G	personal computer, supporto cartaceo
10	Manutenzione hardware degli strumenti utilizzati per il trattamento dei dati	C, S, G	personal computer, supporto cartaceo
11	Gestione tecnica operativa (backup, ripristino, verifica backup)	C, S, G	personal computer, supporto cartaceo

Per tutte le banche dati detenute dall'Ente i trattamenti che vengono effettuati dagli operatori sono quelli ricompresi nella precedente tabella, con esclusione degli identificativi 9, 10 e 11, riservate alle attività di manutenzione da eseguirsi a cura del personale all'uopo individuato.

Gli archivi elettronici per la titolarità dell'ente risiedono su server e personal computer operanti in ambiente operativo Microsoft Windows (varie versioni e release) e in ambiente operativo Linux (varie versioni e release); la conservazione delle copie di backup avviene in ambienti separati da quelli di operatività dei server.

Gli archivi cartacei sono suddivisi, a norma delle leggi a presidio della materia, tra archivio

corrente, storico e di deposito posto nel piano interrato della Sede comunale e le varie Unità Operative (nel seguito: U.O.) per le pratiche in itinere e quelle inerenti le pratiche esaurite in attesa di essere avviate all'archivio generale come sopra individuato.

Si precisa che ogni U.O. provvede al rispetto delle norme di sicurezza previste al successivo articolo 2.

Art. 2. Conservazione dei documenti e mezzi in dotazione all'Ente

La conservazione dei documenti viene effettuata in ossequio alle vigenti leggi, a tutela della integrità degli stessi e della tutela della riservatezza, con idonei mezzi di protezione sia fisici sia elettronici.

In particolare la documentazione cartacea inerente a dati definiti sensibili dal D.Lgs. 196/2003 viene conservata in apposite cartelle personali contenute in armadi o classificatori dotati di chiusura con chiave; in difetto il locale ove sono conservati i dati è accessibile solo alla presenza degli addetti all'Ufficio. In difetto il locale è chiuso a chiave.

Particolare e più attenta procedura viene seguita per la gestione della documentazione personale dei dipendenti, in particolare la stessa viene gestita con le cautele di cui alla disposizione dl Garante del 17 ottobre 2004, sia per quanto concerne i trattamenti cartacei sia per quanto concerne i trattamenti con mezzi elettronici.

Per quanto concerne la dotazione informatica dell'Ente si precisa che, allo stato attuale lo stesso dispone di:

- una rete cablata presso la sede comunale centrale di via Carlo Cattaneo 1
- una rete cablata presso la sede distaccata di via A. De Gasperi 3 ove opera il Comando della Polizia locale
- uno sportello distaccato in via Mozart 45
- 33 server (tra fisici e virtuali) alloggiati nella sala server di via Cattaneo 1, sui quali risiedono le banche dati utilizzate dai personal computer client
- 140 personal computer (circa) in funzione di client dai quali il dipendente personale gestisce i processi dell'Ente.

Si precisa che tutti i PC sono dotati di password di accesso al sistema operativo, alla rete aziendale e alle singole procedure come da requisito minimo di sicurezza di cui all'allegato B al D.Lgs. 196/2003.

All'interno degli uffici comunali vengono utilizzati numerosi software per il trattamento dei dati; nella tabella che segue vengono elencati le principali applicazioni installate su personal computer e server, escludendo dall'elenco tutto il software di base facente parte del sistema operativo.

codice	nome	produttore	funzione principale
1	Primus (famiglia)	ACCA	contabilità lavori pubblici
2	Cf4 (famiglia)	ADS	contabilità, mutui, fatturazione
3	Gs4 (famiglia)	ADS	atti, protocollo
4	Tr4 (famiglia)	ADS	fiscalità locale
5	De4 (famiglia)	ADS	servizi demografici, elezioni, S.A.I.A.
6	Ci4	ADS	cespiti e inventario
7	Gc4 (famiglia)	ADS	economo e cassa economale
8	Gre	ADS	rette scolastiche
9	Cim2000	Grafiche Gaspari	cimiteri
10	Sigepro	In.i.t.	commercio
11	JobTime	Infoline	presenze del personale
12	Alice	Maggioli	pratiche edilizie
13	Polcity	Open Software	verbali per le infrazioni del codice della strada
14	Mc3	Proveco	albo pretorio, notifiche
15	Piemme (famiglia)	Sapignoli	verbali per le infrazioni del codice della strada, rapporti incidenti stradali
16	LibreOffice	The Document Foundation	produttività individuale: elaborazione testi, foglio di calcolo, gestione di database, presentazioni, redazione stampati

Dettaglio produttori:

- ACCA software S.p.a. - Via M. Cianciulli, 114 - 83048 Montella
- ADS automated data systems S.p.a., Via del lavoro, 17 - 40127 Bologna
- Grafiche E. Gaspari S.r.l. - Via M. Minghetti, 18 - 40057 Cadriano
- In.I.T. S.r.l. - Via N. Bixio, 45 - 06135 Perugia
- Info Line S.r.l. - Via Emilia, 72 - 43010 Castelguelfo di Fontevivo
- Maggioli S.p.A. - Divisione ELDASOFT - Via E. Reginato, 87 – 31100 Treviso
- Open Software S.r.l. - Via G. Galilei, 2/C/2 - 30035 Mirano
- Proveco S.r.l. - Via O. Rinuccini, 38 - 50144 Firenze
- Sapignoli S.r.l - Via Molino Vigne, 2 - 47825 Torriana
- The Document Foundation - Kurfürstendamm 188 - 10707 Berlin - Germany

L’Ente ha predisposto una rete di videosorveglianza gestita dal personale della Polizia Locale.

La Centrale Operativa è ubicata in locale dedicato che in assenza di presidio da parte dall’operatore rimane chiuso; il locale non è accessibile direttamente dall’esterno e non è visibile

dal pubblico.

Nella Centrale Operativa esistono i monitor di sorveglianza e presso la stessa, in apposito contenitore chiuso, devono essere conservati i supporti di ripresa con le immagini per il tempo non superiore a quello in linea generale prescritto dal Garante con il provvedimento del 29 aprile 2004 e stabilito dal Regolamento comunale sulla videosorveglianza.

L'impianto di videosorveglianza, è conforme alle disposizioni emesse del Garante con il provvedimento 29 aprile 2004 dal medesimo emanato, nonché di tutte le altre incombenze previste dalla legge, e sono stati assolti gli incombenti di informazione alla generalità dell'utenza prima dell'avvio della operatività.

Si segnala che sono state posizionate apposite tabelle di avviso, secondo disposizioni del Garante, in prossimità delle videocamere attivate al fine della comunicazione di "area videosorvegliata".

Decorso il termine stabilito dal Regolamento comunale sul trattamento dei dati acquisiti con il sistema di videosorveglianza avverrà d'ufficio la cancellazione delle immagini a meno che non ricorrano i casi previsti dalla legge ed evidenziati specificatamente nella disposizione regolamentare.

Art. 3 Analisi dei rischi

L'analisi dei rischi, effettuata a seguito di controlli e sopralluoghi effettuati sia nella sede centrale dell'Ente si in quelle periferiche, ha evidenziato le seguenti possibilità:

- alterazione, danneggiamento, distruzione accidentale o dolosa del sistema, dei programmi e dei dati
- trattamento, diffusione, comunicazione dei dati non autorizzata sia accidentale sia dolosa
- danneggiamento delle risorse informatiche per disastri naturali (incendi, infiltrazione d'acqua)
- accessi non autorizzati alle apparecchiature ed ai dati
- sottrazione di elaboratori, programmi, supporti o dati.

L'analisi dei rischi ha pertanto evidenziato la necessità di predisporre misure di sicurezza relative a:

- sicurezza fisica, quali ad esempio il furto e il danneggiamento delle apparecchiature informatiche
- sicurezza logica, quali ad esempio gli accessi ai computer, alla rete e alle banche dati.

Nelle tabelle che seguono si elencano le tipologie di rischi individuate.

Rischi relativi ai locali

codice	descrizione sintetica del rischio	impatto sulla sicurezza	rischio
A001	Accesso non autorizzato ai locali	Danneggiamento dei macchinari, dei dati, delle strutture e dei supporti cartacei	basso
A002	Furto	Perdita dei macchinari contenenti i dati e/o delle banche dati cartacee	basso
A003	Eventi naturali o non direttamente provocati dall'uomo (incendio, allagamento, terremoto, meteorite)	Distruzione delle banche dati e degli strumenti	medio

Rischi relativi agli strumenti utilizzati

codice	descrizione sintetica del rischio	impatto sulla sicurezza	rischio
B001	Uso non autorizzato dell'hardware	Danneggiamento delle procedure trattamento dati	Medio
B002	Guasto	Momentanea impossibilità del trattamento dati	Medio
B003	Rischi connessi all’elettricità	Danneggiamento dell'hardware e delle procedure trattamento dati	Alto
B004	Accesso non autorizzato ai locali	Danneggiamento materiale cartaceo	Basso

Rischi relativi al software

codice	descrizione sintetica del rischio	impatto sulla sicurezza	rischio
C001	Presenza di bugs nel software	Non corretto funzionamento trattamento dati	Medio
C002	Presenza di virus informatici	Non corretto funzionamento trattamento dati, cancellazione procedura trattamento dati, disfunzioni alla banca dati trattata	Medio
C003	Presenza di spyware	Violazione delle chiavi di autenticazione ed autorizzazione verso l'esterno	Basso
C004	Utilizzo non autorizzato del software	Cancellazione e/o modifica di dati all’interno di banche dati custodite	Basso
C005	Software non aggiornato	Non corretto funzionamento trattamento dati	Basso
C006	Cattivo utilizzo del software	Non corretto funzionamento trattamento dati	Basso

Rischi relativi alle banche dati

codice	descrizione sintetica del rischio	impatto sulla sicurezza	rischio
D001	Accesso non autorizzato	Cancellazione e/o modifica dei dati personali su banche dati protette	Medio
D002	Perdita dati	Perdita della banca dati	Basso

Art. 4 Misure adottate e da adottare per l’integrità e la sicurezza del sistema

Dall’analisi dei rischi è emersa la necessità di mettere in atto alcune misure destinate all'integrità del sistema.

4.1 Autenticazione al sistema informatico comunale

Avviene attraverso un codice identificativo univoco non riutilizzabile e una parola chiave con lunghezza di almeno 8 caratteri alfanumerici che deve essere cambiata dall'utente almeno ogni 84 giorni. Al fine di rendere operativa questa misura, alla scadenza del termine indicato il sistema informatico non consente all'utente l'accesso fino al cambio della password.

4.2 Programma antivirus

È installato su tutti gli elaboratori (sia server che client) e viene aggiornato automaticamente almeno una volta al giorno; controlla tutto il sistema informativo comunale compresa la posta elettronica.

4.3 Trattamento dati cartacei

Vengono eseguiti i seguenti controlli:

- la validità delle richieste di accesso ai dati personali è verificata prima di consentirne l'accesso
- gli atti e i documenti contenenti i dati vengono conservati in archivi ad accesso selezionato e, se affidati agli incaricati, vengono da questi ultimi conservati e restituiti al termini delle operazioni affidate
- il titolare e il responsabile, nel designare gli incaricati, autorizza preventivamente per iscritto il solo accesso ai dati la cui conoscenza sia strettamente necessaria all'adempimento dei compiti assegnati
- gli atti e i documenti contenenti i dati, se affidati agli incaricati del trattamento, vengono conservati fino alla restituzione in contenitori muniti di serratura
- l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura: l'adempimento di tale prescrizione si concreta nel consentire l'accesso agli archivi oltre l'orario di chiusura solo ed esclusivamente al responsabile del trattamento o ad un suo incaricato
- eventuali supporti informatici di memorizzazione (nastri magnetici, cassette, dischi magnetici o ottici rimovibili, cd-rom, chiavette USB) contenenti la riproduzione di informazioni relative al trattamento di dati personali di cui al D. Lgs. 196/2003 vengono conservati in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave
- il controllo dei documenti stampati o fotocopiati è responsabilità degli incaricati al trattamento: la stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti ad accesso controllato o presidiati dall'incaricato.

4.4 Misure di sicurezza per i locali dove sono alloggiati i server

Qualora non siano presenti gli operatori del servizio informatico, i server sono tenuti chiusi a chiave in un locale idoneo, opportunamente climatizzato e dotato di gruppo di continuità elettrica; a tale locale è consentito l'accesso solo personale espressamente autorizzato.

4.5 Misure di sicurezza all'atto dell'entrata e dell'uscita

I dipendenti sono tenuti a segnalare la propria presenza tramite l'utilizzo di badge magnetico personale in dotazione. Tale badge magnetico è stato assegnato anche agli amministratori comunali. Sono in fase di attuazione le misure a presidio e garanzia a beneficio delle figure

professionali che accedono alla struttura a titolo di consulenza. Particolare attenzione viene posta alla sezione dedicata al Servizio Anagrafe, Elettorale, Stato civile e Leva per le implicazioni e le maggiori cautele derivanti dall'osservanza delle ulteriori prescrizioni per l'emissione della Carta d'Identità Elettronica. L'accesso degli uffici al pubblico avviene solo previo riconoscimento dell'utente ad eccezione dell'accesso allo Sportello del Cittadino e degli Uffici decentrati.

4.6 Misure antincendio.

Le sedi comunali sono dotate di estintori quali dispositivi antincendio e degli altri presidi stabiliti dall'apposito piano di sicurezza redatto ai sensi della legislazione in materia vigente e a cui si rimanda.

4.7 Misure di allarme in caso di effrazione

Le sedi comunali sono dotate di sistema di allarme inserito automaticamente ovvero dal custode, se presente nell'edificio.

4.8 Backup dei dati informatici

Ogni notte sono programmati salvataggi di tutti i dati gestiti centralmente dal sistema informativo comunale.

I file di backup vengono conservati in sede diversa da quella di residenza dei server.

Per ogni salvataggio viene verificata la correttezza dell'esecuzione e prodotto un file di riepilogo relativo al dettaglio delle operazioni.

La corretta esecuzione dei salvataggi giornalieri viene verificata ogni mattina.

4.9 Le macchine critiche

I server sono alloggiati in un locale apposito a cui può accedere solo il personale del S.I.C.

Tutte le apparecchiature elettriche presenti nel locale server sono collegate ad un gruppo di continuità che ne garantisce per un discreto tempo il funzionamento anche in caso di distacco di corrente dall'intero edificio comunale.

In caso questi casi il sistema provvede ad inviare email di allerta in modo da permettere al personale del S.I.C. di intervenire in modo adeguato.

Le sala server è climatizzata ed è presente un sistema di monitoraggio della temperatura.

4.10 La rete informatica comunale

La sede comunale di via Cattaneo 1 è collegata con il mondo esterno tramite linea dati con tecnologia XDSL.

Il collegamento tra la sede principale di via Cattaneo e quella di via De Gasperi è garantito da un collegamento tramite fibra ottica di proprietà comunale; quello con lo sportello decentrato di via Mozart 45 è garantito da un collegamento via rete telefonica MPLS.

Il collegamento è protetto da eventuali attacchi esterni attraverso un sistema di firewall applicato ai router.

Oltre al firewall è installato un programma di sicurezza che controlla tutte le richieste in entrata dal mondo esterno in modo da impedire la penetrazione non autorizzata nel sistema utilizzando determinato servizi e/o protocolli di rete.

Il programma controlla anche la presenza di eventuali virus nella posta elettronica in ingresso e

impedisce la navigazione in alcune categorie di siti internet potenzialmente pericolose.

Altre sedi/uffici comunali possono essere collegate al sistema informatico utilizzando le modalità di collegamento già in essere oppure attraverso internet, utilizzando servizi terminali opportunamente configurati per garantire un adeguato livello di sicurezza.

Al sistema informativo comunale possono accedere anche altri Enti Pubblici utilizzando collegamenti punto-punto oppure attraverso internet utilizzando servizi terminali opportunamente configurati per garantire un adeguato livello di sicurezza.

Questo tipo di connessione viene configurato solo per la consultazione delle banche dati.

4.11 Servizi esternalizzati

Per aumentarne il livello di sicurezza, il web server relativo al sito comunale ed il mail server relativo alla posta elettronica del dominio "comune.pioltello.mi.it" non sono residenti all'interno della rete informatica comunale ma operano sui server di un gestore esterno.

Il server di posta elettronica interno è protetto da un sistema antivirus.

4.12 Misure in essere e da adottare per i locali

codice rischio	locali	misura	in essere	da adottare	periodicità controllo
A001	tutti	ingresso controllato dal personale	sì		6 mesi
A002	tutti	cartaceo chiuso in armadi con serratura o in locale chiuso con serratura	sì		6 mesi
A003	tutti	allarme centralizzato	sì		6 mesi
A004	tutti	vigilanza notturna accessi e struttura	sì		6 mesi
A005	sala server	chiusura a chiave	sì		6 mesi
A006	tutti	estintori	sì		6 mesi (D. Lgs 81/2008)

4.13 Misure in essere e da adottare per gli strumenti utilizzati

codice rischio	strumenti	misura	in essere	da adottare	periodicità controllo
B001	personal computer	digitazione password all'accensione del pc	sì		6 mesi
B002	personal computer	i pc hanno in essere un contratto di manutenzione o garanzia	sì		6 mesi
B003	personal computer	i pc sono protetti da un sistema di UPS	no		6 mesi
B004	cartaceo	cartaceo è chiuso in faldoni all'interno di un armadio chiuso a chiave o in stanza chiusa a chiave	sì		6 mesi

4.14 Misure in essere e da adottare per i software utilizzati

codice rischio	software	misura	in essere	da adottare	periodicità controllo
C001	tutti i programmi software elencati al precedente articolo 2	per i software gestionali vi è un contratto di assistenza	sì		6 mesi
C002	G Data antivirus	presenza di antivirus aggiornato	sì		6 mesi
C003	Telecom - rete Interbusiness	presenza di firewall e apparato finalizzato alla la verifica degli accessi verso l'esterno	sì		6 mesi
C004	tutti i programmi software elencati al precedente articolo 2	per accedere esiste password di autenticazione	sì		6 mesi
C005	tutti i programmi software elencati al precedente articolo 2	la ditta con cui si ha il contratto di assistenza comunica gli aggiornamenti	sì		6 mesi
C006	tutti i programmi software elencati al precedente articolo 2	gli utenti conoscono bene le procedure per la gestione dei dati	sì		6 mesi

4.15 Misure in essere e da adottare per le banche dati

codice rischio	banca dati	misura	in essere	da adottare	periodicità controllo
D001	tutti i programmi software elencati al precedente articolo 2	per accedere esiste password di autenticazione	sì		6 mesi
D002	tutti i programmi software elencati al precedente articolo 2	i dati risiedono su server con backup giornaliero	sì		6 mesi

Art. 5 Criteri e modalità del ripristino dei dati

Dei dati gestiti dal sistema informatico viene fatta periodicamente copia di sicurezza come specificato nel precedente articolo (si veda articolo 4.8).

La tipologia della strumentazione utilizzata per la gestione delle informazioni condivise consente di risolvere le seguenti problematiche:

- cali e/o sbalzi di tensione e brevi blackout, attraverso appositi gruppi di continuità (si veda articolo 4.9)
- danneggiamento di hardware, attraverso apposita configurazione che consente di limitare i danni derivanti da questa tipologia di rischi e condizionamento dei locali (si veda articolo 4.9)
- malfunzionamenti del software con contratti di assistenza (relativi alle procedure maggiormente critiche).

Per quanto riguarda il ripristino dei dati, esso si suddivide nelle seguenti procedure:

- il recupero dei singoli file avviene di norma entro il giorno lavorativo successivo alla richiesta di intervento
- il recupero di banche dati e programmi avviene di norma entro i due giorni lavorativi successivi alla richiesta di intervento
- il ripristino completo del sistema con il recupero dei dati è previsto di norma entro i cinque giorni lavorativi successivi alla richiesta di intervento.

Art. 6. Titolare, Responsabili e incaricati

Per la definizione dei compiti e delle prerogative delle dette figure si effettua espresso rinvio agli articoli 3,4 e 5 del "Regolamento comunale per il trattamento dei dati personali".

Sono state effettuate specifiche nomine per le figure individuate amministratore di sistema, come disposto dalla decisione del Garante del 27 novembre 2008 pubblicata in G.U. n. 300 del 24-12-2008.

Si specifica che vengono effettuate periodiche verifiche almeno annuali sull’operato come da

disposizioni del Garante.

Art. 7. Formazione degli operatori e delle figure autorizzate ad accedere nel sistema

L'Ente predispone degli appositi interventi periodici per la formazione delle figure che hanno autorizzazione di accesso alle banche dati detenute presso l'Ente al fine di evitare dispersione di dati ed accessi indebiti. La formazione è continua, per cui vengono periodicamente previsti degli interventi aggiuntivi rispetto al modulo di base a cui ha partecipato la quasi totalità degli operatori interni.

La formazione di base riguarda il processo di autenticazione con particolare riferimento a:

- le regole generali di autenticazione, rappresentate dall'identificazione univoca dell'utente attraverso la coppia: codice identificativo + password
- la frequenza di cambiamento della password e non ripetibilità della stessa neanche in tempi successivi
- l'attribuzione univoca del codice identificativo che risulta non assegnabile a nessun altro utente neanche in futuro
- l'immediata sostituzione della password dopo un accesso forzato da parte di personale all'uopo autorizzato nei casi di necessità e di urgenza ed in assenza del titolare
- le diverse regole di autenticazione per l'accesso ai dati sensibili e /o giudiziari
- le modalità di conservazione della documentazione
- la riservatezza dei dati e delle notizie di cui si viene a conoscenza
- i metodi ed i mezzi di archiviazione della documentazione in maniera da tutelare e garantire il diritto alla riservatezza dei cittadini e degli utenti
- le modalità di consegna dei documenti e di intervento telefonico verso cittadini ed utenti al fine di evitare eventuali comunicazioni involontarie di notizie riservate
- le nozioni per evitare di cadere in fenomeni di social engineering , fishing, ecc.

I periodici momenti formativi permetteranno agli operatori di avere sempre una conoscenza aggiornata alle necessità per la adeguata trattazione dei dati.

In particolare sono previsti degli interventi per allineare, almeno per principi fondanti, le nuove norme emanate e che sono da affrontare unitariamente tra diritto di accesso e tutela della riservatezza dei dati.

Per il personale neo assunto, per gli incaricati esterni e per i lavoratori a contratto e per le persone che effettuano degli stages, sono previste particolari e riservate sessioni formative finalizzate all'assolvimento del compito assegnato conformemente allo spirito della norma giuridica e secondo quanto disposto dalla regolamentazione esistente dell'Ente.

Art. 8 Trattamenti esterni

L'Ente si avvale delle seguenti ditte in supporto alle proprie attività:

- ACCA software S.p.a. - Via M. Cianciulli, 114 - 83048 Montella
- ADS automated data systems S.p.a., Via del lavoro, 17 - 40127 Bologna

- Grafiche E. Gaspari S.r.l. - Via M. Minghetti, 18 - 40057 Cadriano
- In.I.T. S.r.l. - Via N. Bixio, 45 - 06135 Perugia
- Info Line S.r.l. - Via Emilia, 72 - 43010 Castelguelfo di Fontevivo
- Maggioli S.p.A. - Divisione ELDASOFT - Via E. Reginato, 87 – 31100 Treviso
- Open Software S.r.l. - Via G. Galilei, 2/C/2 - 30035 Mirano
- Proveco S.r.l. - Via O. Rinuccini, 38 - 50144 Firenze
- Sapignoli S.r.l - Via Molino Vigne, 2 - 47825 Torriana

Le sopraelencate ditte, per funzioni collegate al mantenimento ed alla manutenzione degli archivi, possono avere accesso alle banche dati mantenute sui server e sui personal computer client comunali in modalità presidiata.

Le operazioni di accesso ai dati avvengono, di norma, su richiesta del personale del servizio informatico comunale e sono previste e regolate dai contratti di assistenza software in essere tra il Comune di Pioltello e le singole aziende.

Per il trattamento dei dati da parte delle elencate Ditte, i contratti di servizio e di assistenza prevedono espressa assunzione di responsabilità per le operazioni dalle stesse effettuate. Per quanto concerne gli standard e le procedure di sicurezza si rimanda ai singoli documenti delle rispettive ditte.

Art. 9 Contenuti del documento: parte programmatica e sua attuazione

Il presente documento è composto sia da una parte che rileva l’esistente sia da una serie di disposizioni programmatiche che troveranno attuazione nel corso di validità del documento stesso.

In particolare l’Ente intraprenderà le opportune azioni al fine di adeguare le proprie strutture informatiche a quanto disposto dal Codice sulla digitalizzazione nella P.A., al fine di:

- evitare l’accesso agli sportelli da parte degli utenti per la presentazione di documenti cartacei o per firmare personalmente domande o istanze o per fornire chiarimenti, rendendo disponibile un canale digitale sicuro e certificato
- rendere disponibili agli utenti atti e procedimenti in modo sicuro e trasparente in formato digitale e nel rispetto della normativa vigente per il rispetto dei dati personali
- rendere possibile i pagamenti in forma digitale dalla data prevista dal Codice medesimo
- effettuare le comunicazioni all’indirizzo di posta elettronica dichiarato dagli utenti che ne faranno richiesta con l'avvertenza che la trasmissione delle informazioni, se effettuata attraverso un canale di posta elettronica certificata e con apposizione di firma digitale, avrà pieno valore legale a norma di legge
- organizzare i servizi in modo da controllare periodicamente la qualità e la soddisfazione dell’utenza
- rendere disponibili in rete entro il termine fissato dal Codice moduli e formulari con la possibilità di compilazione dei medesimi senza la loro trasformazione in documento cartaceo.

A tal fine è stata approvato dalla Giunta Comunale con delibera n. 21/2015 - a cui si rinvia - il Piano di informatizzazione delle procedure dell'ente che - per espressa previsione inserita nei documenti di programmazione dell'ente - è obiettivo di performance organizzativa e individuale.

Art. 10 Note, disposizioni di rinvio

Si allegano le diverse deliberazioni che l'ente ha adottato negli anni in materia di privacy e tutela dei dati personali.

Si specifica che fin dal 2008 l'Ente adotta norme di comportamento per il corretto utilizzo dei sistemi informatici aziendali e delle banche dati (allegato 1, con pieno valore attuale).

Pioltello, 23 NOV 2015

Il Dirigente del Settore Affari Generali
(Dott. Andrea Novaga.)

Allegato 1 - "Norme per il corretto utilizzo dei sistemi informatici aziendali e delle banche dati"

(Versione 2.0 del 19 novembre 2015, a modifica della versione 1.5 del 27 maggio 2008)

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza - atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro o rapporto professionale o altro titolo con cui si accede legittimamente alle risorse aziendali - si ritiene utile adottare alcune regole interne di comportamento comune dirette ad evitare comportamenti inconsapevoli e/o scorretti.

Nel rendere pubbliche queste regole, si sottolinea che la loro non osservanza può comportare sanzioni disciplinari, civili e penali.

Oggetto e campo di applicazione del documento

La progressiva diffusione delle nuove tecnologie informatiche espone il Comune a rischi di un coinvolgimento sia patrimoniale sia penale creando al contempo problemi di immagine e sicurezza.

Per far fronte a ciò l'Amministrazione comunale ha già provveduto - con riferimento alle misure di sicurezza imposte per il trattamento di dati personali dalla normativa vigente ed in particolare dal Decreto legislativo 30 giugno 2003, n. 196, integrate opportunamente dalle "Best Practices" e dai "Common Criteria" che sono a fondamento della corretta gestione delle informazioni e della sicurezza sia in campo informatico sia in campo fisico - a fornire a tutti gli utenti dei sistemi informatici idonee indicazioni ed istruzioni, cui dovranno responsabilmente conformarsi.

Per tale ragione il presente documento deve essere portato a conoscenza di tutti gli utenti dei sistemi informatici e delle banche dati del comune; a tale fine viene reso disponibile anche sulla rete aziendale, nel sito dell'Ente e viene affisso all'Albo Pretorio a tempo indeterminato.

Tutti i contratti che verranno conclusi tra l’Ente e terzi soggetti a cui viene permesso l’accesso ai dati, ai programmi informatici o ad altri mezzi dell’Ente, dovranno riportare una clausola che impegni gli utenti a rispettare il presente documento; ciò indipendentemente dalla nomina a incaricato o a responsabile del trattamento dati ai sensi del Decreto legislativo 30 giugno 2003, n. 196.

Nel caso di un utente esterno nominato responsabile del trattamento, questi deve impegnarsi a far rispettare il presente documento a tutti i propri dipendenti e ad eventuali altri soggetti a lui correlati.

Si precisa che sono considerati utenti tutti i soggetti, qualunque sia il loro status, che possono validamente accedere, consultare, creare o gestire le risorse informatiche dell'Ente.

I sistemi informatici aziendali: generalità

Il personal computer (fisso o mobile, comprese le periferiche ad esso connesse) ed i relativi programmi e/o applicazioni sono di proprietà del Comune e vengono affidati al dipendente, al professionista collaboratore o ad altra personalità con titolo ad accedere, quali strumenti di lavoro.

Pertanto tali strumenti:

- vanno custoditi in modo appropriato
- possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali o illeciti
- Il furto, il danneggiamento o lo smarrimento di tali strumenti debbono essere prontamente

segnalati al dirigente dell'area di lavoro.

Gli strumenti informatici nel loro complesso - personal computer, periferiche, telefonini evoluti, ecc. - sono utilizzati dai dipendenti (a qualsiasi livello e con qualunque tipo di contratto), dagli Amministratori e da tutte le persone che, anche in forza di contratti di consulenza e collaborazione temporanea, accedono alla rete informatica comunale per il trattamento dei dati propri dei singoli uffici e delle singole mansioni.

Il trattamento dei dati deve seguire le norme di sicurezza previste dall'apposito Documento Programmatico sulla Sicurezza (DPS) aziendale, già illustrato in altre sedi ed al quale si rimanda per quanto non esplicitato in questo documento.

L'Ente si adopera e persegue il fine di proteggere con le tecniche più moderne ed avanzate sia gli utenti sia le risorse messe a loro disposizione contro ogni rischio potenzialmente prevedibile, secondo le regole di buona tecnica contenute nelle norme e tecniche di sicurezza applicate nell'Ente nonché nelle disposizioni legislative in materia.

L'Ente definisce un piano di gestione della documentazione con l'adozione di standard riconosciuti universalmente idonei a garantire la sicurezza delle informazioni, con particolare attenzione alla trattazione dei dati sensibili e giudiziari.

I sistemi informatici aziendali: modalità di utilizzo

Ai fini sopra esposti vengono nel seguito richiamati i principali atti o comportamenti da adottare e/o da evitare, con l'avviso che l'elenco seguente è solo indicativo e certamente non esaustivo.

Accesso alla rete ed alle procedure

1. L'accesso alla rete aziendale ed alle procedure software in uso nei singoli uffici è regolato da un sistema che prevede l'utilizzo di una doppia chiave: "nome utente" e "password" (credenziali).

   Al primo accesso, ad ogni utilizzatore della rete aziendale viene assegnato il proprio "nome utente" ed una "password" generica, con lo specifico obbligo di modifica immediata di quest'ultima.

   Le "password" di accesso alle rete aziendale hanno una durata temporale limitata, al termine della quale non sono più utilizzabili.

2. Ad ogni accesso alla rete aziendale ed alle diverse procedure ogni utente è tenuto ad utilizzare unicamente il "nome utente" a lui assegnato con la propria "password".

   Non è consentito l'utilizzo di "nomi utente" collettivi ed è vietato l'utilizzo di "nomi utente" di altre persone anche con l'esplicito consenso delle stesse.

3. L'accesso alle strutture informatiche aziendali è limitato temporalmente nell'arco della giornata e nell'arco della settimana.

4. L'accesso del dipendente alla rete aziendale attraverso le proprie credenziali è finalizzato all'utilizzo delle risorse proprie dell'ufficio di appartenenza e per le funzioni al dipendente assegnate; ogni altro utilizzo delle proprie credenziali di accesso alla rete aziendale è pertanto espressamente vietato.

Le limitazioni sono stabilite in base alle informazioni ed alle richieste della Direzione e sono messe in atto dal personale autorizzato dal Responsabile del servizio informatico comunale (nel seguito "personale IT").

Utilizzo del personal computer

1. Onde evitare il grave pericolo di introdurre virus informatici, codici malevoli e/o altre entità che possano attentare all'integrità dei dati e delle risorse nonché alterare la stabilità delle applicazioni dell'elaboratore, non è consentito installare programmi se non espressamente autorizzati dal personale IT. Non è consentito inoltre l'uso di programmi non distribuiti ufficialmente e dei quali il Comune non detenga regolare licenza d'uso.
2. Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici.
3. Non è consentito modificare le configurazioni impostate sul proprio PC né reinstallare o alterare il sistema operativo o qualsiasi altro software fornito in dotazione. Non è consentito avviare il personal computer tramite supporti esterni e con sistemi operativi diversi da quelli installati dal personale IT.
4. Non è consentito smontare, modificare o manomettere in alcun modo l'hardware del PC o delle periferiche ad esso connesse o direttamente collegate alla rete dati aziendale, se non limitatamente alle operazioni strettamente legate al normale uso dell'apparecchiatura stessa (come, ad esempio, rimuovere parti della stampante per eliminare inceppamenti carta o sostituire cartucce di stampa o toner).
5. Non è permesso spostare apparecchiature informatiche "fisse" o scambiare periferiche tra diversi PC senza autorizzazione del personale IT.
6. Non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio modem, cellulari ecc.) se non autorizzati dal personale IT e comunque sotto la sua supervisione.
7. Non è consentito il salvataggio di file personali o non attinenti all'attività lavorativa sul personal computer aziendale; in ogni caso il Comune non è da ritenersi responsabile per la perdita o per l'uso da parte di chicchessia di tali informazioni, sia per cause accidentali sia per attività di manutenzione ordinaria e straordinaria sull'hardware ad opera del personale IT.

Utilizzo di supporti di memorizzazione esterni

1. Non è consentito scaricare files contenuti in supporti di memorizzazione esterni o in generale introdurre files nella rete aziendale se essi non hanno attinenza con la propria prestazione lavorativa.
2. Tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo antivirus prima dell'utilizzo. In caso di segnalazioni provenienti dal sistema di controllo antivirus, il file non deve in alcun modo essere utilizzato e deve essere immediatamente informato il personale IT.
3. Non è consentito esportare file di qualunque genere dalle apparecchiature delle rete aziendale a supporti destinati all'utilizzo al di fuori di essa (quali cd, dvd, chiavi USB, hard disk esterni, ecc.) senza l'esplicita autorizzazione da parte del proprio dirigente o responsabile. In ogni caso l'esportazione di tali file dovrà avvenire mettendo in funzione i necessari sistemi di cifratura atti ad impedirne la visione o l'utilizzo da parte di terzi non autorizzati come, ad esempio, in caso di furto o smarrimento del supporto di memorizzazione. Lo stesso divieto è valido per l'invio di file attraverso sistemi di posta elettronica o servizi di salvataggio file "in cloud".

Utilizzo delle risorse della rete aziendale

1. Le unità di rete 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 in queste unità nemmeno per brevi periodi.

2. Salvo diversa ed espressa indicazione del personale IT, tutti i file di utilizzo professionale devono essere salvati sulle unità di rete, in quanto esse sono oggetto di periodiche operazioni di salvataggio su dispositivi sicuri.
3. Il Comune si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente documento senza alcun preavviso o comunicazione all'utente proprietario di detti file o applicazioni.
4. Senza l'autorizzazione del personale IT è vietato il collegamento alle strutture ed alle apparecchiature della rete aziendale di qualunque tipo di componente hardware che non sia di proprietà comunale.

Utilizzo della rete Internet, dei collegamenti con l'esterno e dei relativi servizi

Navigazione in Internet

1. Non sono permesse, a meno di specifiche e documentate autorizzazioni, le seguenti attività:

a) caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse dell'Ente documenti, informazioni, immagini, filmati, ecc. :

- carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate
- pregiudizievoli per le risorse dell'Ente e per l'integrità e la conservazione dei dati dell'Ente stesso
- pregiudizievoli per l'immagine e il buon nome dell'Ente all'esterno dell'Ente

b) accedere a server web trattanti materie o soggetti ricadenti in soggetti rientranti nelle categorie sopra elencate

c) utilizzare le risorse dell'Ente con fini di molestia, minaccia o comunque violando le norme di legge in vigore

d) caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure od altra utilità che siano protetti dalle leggi sulla proprietà intellettuale, salvo che il Comune di Pioltello ne detenga regolare licenza e/o autorizzazione del produttore

e) utilizzare strumentazioni, programmi, software, procedure, ecc. messi a disposizione dall'Ente in violazione delle Leggi sulla proprietà intellettuale, delle regole di buona tecnica applicabili e delle prescrizioni emanate dall'Ente

f) caricare o trasmettere, con volontà, archivi o programmi contenenti virus o dati alterati

g) manomettere l'integrità dei dati

h) utilizzare le risorse dell'Ente in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla Legge e dai Regolamenti.

Poiché alcune attività sopra elencate possono avere conseguenze di natura penale, esse

originano in capo al trasgressore tutte le responsabilità previste dalla Legge.

L’Ente si riserva il diritto di effettuare verifiche e controlli regolari, con le garanzie ed i limiti posti dalla Legge e secondo le prescrizioni emanate dal Garante per la tutela ed il trattamento dei dati personali.

2. Non è consentita l'effettuazione di qualsiasi genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo casi direttamente autorizzati dal dirigente delle risorse informatiche e/o dal responsabile IT e con il rispetto delle normali procedure di acquisto.

3. Non è consentito lo scarico di software e file in genere, anche se gratuiti, prelevati da siti Internet, se ciò non è espressamente autorizzato dal personale IT.

4. È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

5. Non è permessa la partecipazione, per motivi non professionali, a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames).

6. Le attività di "streaming" audio e video tramite le connessioni internet sono vietate.

Posta elettronica

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare quanto segue.

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

2. Al fine di evitare inutile traffico di rete e spreco di spazio e risorse sul sistema di posta non è consentito inviare messaggi a tutti i destinatari della rubrica indirizzi interna (es.: per auguri di Natale, ecc.), salvo non si tratti di comunicazioni importanti e necessarie, o favorire il propagarsi di notizie riconducibili a ciò che comunemente viene definito come “catena di S. Antonio”.

3. La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei: pertanto non deve essere usata per inviare documenti di lavoro "Riservati" o contenenti dati sensibili senza autorizzazione del proprio dirigente; tali messaggi dovranno comunque essere criptati.

4. Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione.

5. In caso di assenza dal posto di lavoro (per ferie, malattia o altro) l'utente della posta elettronica è tenuto ad attivare il messaggio automatico di risposta che segnala la propria indisponibilità a ricevere la posta e che contestualmente comunica agli interlocutori esterni gli indirizzi dei dipendenti presenti nel posto di lavoro durante il proprio periodo di assenza.

6. Poiché la posta elettronica, laddove non utilizzata congiuntamente a specifici dispositivi, non ha valore legale, essa di norma non dovrà essere utilizzata per le comunicazioni aventi carattere ufficiale.

A questo proposito si ricorda che il comune è dotato di una casella di posta elettronica certificata (protocollo@pec.comune.pioltello.mi.it) il cui valore è assimilato alla posta raccomandata con ricevuta di ritorno; questa casella è gestita direttamente dal programma di protocollo ed è utile per le comunicazioni tra gli enti pubblici e con quelle persone, fisiche o giuridiche, che hanno attivo un servizio di posta elettronica certificata.

Sistemi di tutela aziendale

Ferma restando la necessità che i singoli utilizzatori mettano in pratica le disposizioni sopra

impartite, vengono attuate a livello di ente e costantemente monitorate e aggiornate le misure di sicurezza idonee a garantire il massimo livello di sicurezza nell'Ente a norma delle leggi, delle regole ISO e di buona pratica.

Controlli

Poiché in caso di violazioni contrattuali e giuridiche sia il Comune sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni anche di natura penale, nei limiti consentiti dalle norme legali e contrattuali il comune verificherà il rispetto delle regole e l'integrità del proprio sistema informatico, avvalendosi del personale IT, nel rispetto delle disposizioni emanate dal garante in materia e con la procedura che verrà eventualmente concordata con le organizzazioni sindacali.

Tali controlli si configurano principalmente nell'analisi dei "file di log" dei sistemi di controllo del traffico dall'interno della rete aziendale verso il mondo esterno (e viceversa) e nell'analisi dei "file di log" dei sistemi di controllo antivirus.

Questo primo livello di controlli non viene effettuato in modo costante e continuativo ma si limita ad analizzare dati con informazioni organizzate in forma aggregata, senza quindi la possibilità di leggere l'attività individuale dei singoli utenti della rete.

Qualora fossero rilevate violazioni delle regole aziendali, si attiveranno le procedure progressive dettate dal garante in materia di controlli informando altresì tempestivamente il personale interessato, giungendo, se necessario a monitorare l'utilizzo delle risorse messe a disposizione del singolo utente.

Sono fatte salve da detta procedure le ispezioni disposte con ordine dell'Autorità Giudiziaria o dal Garante della Privacy.

Informazioni, dati ed archivi

L’Ente è responsabile della manutenzione tecnica delle risorse messe a disposizione degli utenti e della loro messa in sicurezza; è altresì tenuto a verificare che tutte le apparecchiature informatiche rispondano alle regole giuridiche e tecniche in materia di salute e sicurezza nei luoghi di lavoro.

L’utente è responsabile della conservazione degli archivi, dei dati delle informazioni a propria disposizione, così come degli accessi in visione e/o in modifica che potrebbe consentire a persone terze non dotate di autorizzazione specifica.

Obbligo di segnalazione

Appena ne abbia conoscenza, ogni utente deve prontamente segnalare qualsiasi tentativo di violazione del proprio posto di lavoro o dei propri archivi al responsabile della Sicurezza e/o al Responsabile del Servizio Informatico comunale.

La segnalazione andrà fatta sia per dare tempestivo avvio alle procedure di protezione del sistema, sia per tutelare gli interessi del lavoratore in caso di danni procurati da terzi all’Ente.

Diritto-dovere alla formazione ed all'aggiornamento degli utenti

L’Ente organizza idonei percorsi informativi e formativi al fine di applicare concretamente e correttamente le regole e le prescrizioni di sicurezza previste dal presente documento, nonché dalla normativa vigente in materia di riservatezza dei dati e per la gestione delle informazioni.

L’Ente, prioritariamente a beneficio del personale dipendente, provvede a somministrare apposita formazione, anche in forma specifica e personalizzata, così da accompagnare l’evoluzione delle conoscenze della tecnica e il cambiamento delle procedure impiegate (software, sistemi operativi, ecc).

Ogni utente deve formarsi adeguatamente sulla conoscenza delle tecniche di sicurezza e mantenere il suo livello di conoscenza in linea con il pacchetto di formazione somministrato dall’Ente.

Entrata in vigore

Il presente documento è redatto dall'Ente con la partecipazione delle organizzazioni sindacali, viene consegnato a tutte le lavoratrici e i lavoratori dipendenti, nonché di tutti i soggetti che a diverso titolo lavorano, operano o interagiscono con le procedure e i sistemi dell’Ente, compresi i soggetti che ricoprono cariche istituzionali; esso entra in vigore decorso un congruo termine per l'analisi e le osservazioni eventualmente presentate.

Resta inteso che quanto disciplinato dal presente documento vale solo per il futuro e non può regolare eventi avvenuti prima della sua piena vigenza.

Il presente documento, inoltre, costituisce parte integrante del "Manuale di Organizzazione" in corso di stesura a cura dell'Amministrazione comunale.

Aggiornamento

Il presente documento deve essere aggiornato tempestivamente in caso di mutamento dello stato della tecnica e in caso di modifiche legislative che ne rendano illegittime o obsolete una o più parti.

Deroghe

In deroga alle prescrizioni contenute nei seguenti paragrafi, un utilizzo privato dei mezzi di comunicazione fonici o elettronici dell'Ente è eccezionalmente consentito per far fronte a situazioni documentabili di necessità indifferibile per salvaguardare i diritti fondamentali della persona o di emergenza.

Indice

COMUNE DI PIOLTELLO
PROVINCIA DI MILANO

Codice ente 11063	Protocollo n.
DELIBERAZIONE N. 28 DEL 12/05/2004 Trasmessa al C.R.C. [ ]	

VERBALE DI DELIBERAZIONE DEL CONSIGLIO COMUNALE

OGGETTO: **APPROVAZIONE REGOLAMENTO PER IL TRATTAMENTO E LA TUTELA DEI DATI PERSONALI (PRIVACY)**

L'anno **duemilaquattro** addì **dodici** del mese di **Maggio**, alle ore **21:00**, nella sala delle adunanze, previa osservanza di tutte le formalità prescritte dalla vigente legge, vennero oggi convocati a seduta i componenti il Consiglio Comunale.
All'appello risultano:

DE GASPARI MARIO	P	DI MONTE LUCIA	P
LEPORE ANTONIO	P	COLOPI MAURO	P
PIETROPAOLO GIUSEPPE	P	BINI GERARDO	P
GERVASI COSIMO	**A**	GHIRINGHELLI PAOLA	P
FAZIO FRANCESCO	P	**CAPUSSELA FABIO**	**A**
CAMPANALE MICHELE	P	**COSTANTINO DOMENICO**	**A**
GAIOTTO SAIMON	P	DE CARO STEFANO	P
NOVELLI ROSALIA	P	ALI SEMINARA RENATO	P
CONCAS ANTONIO	P	**CAVALLARO GIUSEPPE**	**A**
DI FONZO FRANCESCO	P	ILARDO PIETRO GIUSEPPE	P
DOTTI CLAUDIO	P	AUREGGI GIULIO LUIGI	P
VECCHIO GIOVANNI	**A**	**NITTI FABIO**	**A**
ZANELLA SILVIO	P	**TORRE ALBERTO**	**A**
VILLANI RAFFAELE	P	**AGNELLI LUCA**	**A**
DE GASPARI EZIO	P	**BASILE RONNIE**	**A**
BOTTASINI GIUSEPPE	P		

Totale presenti 22
Totale assenti **9**

Partecipa all'adunanza il **Segretario Generale Dott. Mario Tarricone** il quale provvede alla redazione del presente verbale.Essendo legale il numero degli intervenuti, il Sig. **Michele Campanale** assume la presidenza e dichiara aperta la seduta per la trattazione dell'argomento indicato in oggetto.

Sono presenti gli Assessori Signori: Negri Francesco Finazzi Walter, Nichetti Antonio, Mazzeo Francesco, Taetti Alberto

Assistono gli scrutatori signori: Di Fonzo Francesco, De Gaspari Ezio, Ghiringhelli Paola.

Discussione:
Omissis…..per la stessa si fa riferimento al processo verbale ricavato dal nastro magnetico inciso durante il dibattito.

IL CONSIGLIO COMUNALE

PREMESSO:

- Che a seguito dell'emanazione del D. Lgs. 196/2003, "Codice sulla tutela dei dati personali" le Amministrazioni debbono, entro il termine perentorio del 30 settembre 2004, dotarsi, tra l'altro, di apposito Regolamento comunale per il trattamento e la tutela dei dati personali (privacy);
- Che il detto Regolamento è parte necessaria ed indispensabile anche per l'adozione di altri documenti fondamentali per il funzionamento dell'Ente, quale il Documento Programmatico sulla Sicurezza, ai sensi del D. Lgs. 196/2003;
- Che il Regolamento in oggetto viene ad assumere, *secundum legem*, la qualifica di Reqolamento di principio, visto che dallo stesso potranno e dovranno discendere le norme di dettaglio che governeranno la *"privacy policy"* dell'Ente;
- Che la bozza di Regolamento in oggetto è stata portata all'esame della Commissione consiliare "Bilancio ed Affari Istituzionali" nella seduta del 21 aprile 2004;
- Che la medesima bozza è stata discussa ed emendata in tale sede;

VISTO:
- Il parere favorevole espresso ai sensi e per gli effetti dell'art. 49 del D. Lgs. 267/2000 in merito alla regolarità tecnica dal Dirigente del Settore Affari Generali;

Vista la dichiarazione dell Dirigente del Settore Contabilità e Programmazione Finanziaria in data 10.5.2004, dalla quale risulta che l'atto non necessita di parere contabile;

- Quanto disposto dal D. Lgs. 196/2003 in merito alla speciale procedura cui sono sottoposti i Regolamenti comunali sulla riservatezza dei dati personali;

Con voti unanimi espressi in modo palese;

DELIBERA

1. di approvare il Regolamento per il trattamento dei dati personali, nel testo che viene allegato alla presente deliberazione;

2. di demandare al Dirigente del Settore Affari Generali le incombenze relative alla trasmissione della presente deliberazione al Garante per la protezione dei dati personali.

Letto approvato e sottoscritto:

IL PRESIDENTE
F.to Michele Campanale

IL SEGRETARIO GENERALE
F.to Dott. Mario Tarricone

CERTIFICATO DI ESECUTIVITA'

Si certifica che la suestesa deliberazione:

- è stata pubblicata nelle forme di legge all'Albo Pretorio del Comune, ove rimarrà esposto per quindici giorni consecutivi dal **17/05/2004** art. 124 D.Lgs. n.267 del 18.8.2000).
-

E' DIVENUTA ESECUTIVA IN DATA: 28/05/2004

[X] – ai sensi dell'art.134 comma 3 del D.Lgs. n.267 del 18.8.2000

IL REGOLAMENTO, DOPO L'ESECUTIVITA' E' STATO RIPUBBLICATO ALL'ALBO PRETORIO PER TRENTA GIORNI CONSECUTIVI, AI SENSI DELL'ART. 9 COMMA 5 DELLO STATUTO COMUNALE

IL SEGRETARIO GENERALE
F.to Dr. Mario Tarricone

Copia conforme all'originale in carta libera per uso amministrativo

Addì

COMUNE DI PIOLTELLO
PROVINCIA DI MILANO

Codice ente 11063	Protocollo n.
DELIBERAZIONE N. 53 DEL 18/10/2005 Trasmessa al C.R.C. [ ]	

VERBALE DI DELIBERAZIONE DEL CONSIGLIO COMUNALE

OGGETTO: **MODIFICA ART 8 ED INTEGRAZIONE DELLA TABELLA A DEL REGOLAMENTO PER IL TRATTAMENTO E LA TUTELA DEI DATI PERSONALI**

L'anno **duemilacinque** addì **diciotto** del mese di **Ottobre**, alle ore **21:00**, nella sala delle adunanze, previa osservanza di tutte le formalità prescritte dalla vigente legge, vennero oggi convocati a seduta i componenti il Consiglio Comunale.
All'appello risultano:

DE GASPARI MARIO	P	DI MONTE LUCIA	P
LEPORE ANTONIO	P	**COLOPI MAURO**	**A**
PIETROPAOLO GIUSEPPE	P	BINI GERARDO	P
GERVASI COSIMO	P	GHIRINGHELLI PAOLA	P
FAZIO FRANCESCO	P	**CAPUSSELA FABIO**	**A**
CAMPANALE MICHELE	P	**COSTANTINO DOMENICO**	**A**
GAIOTTO SAIMON	P	DE CARO STEFANO	P
NOVELLI ROSALIA	P	ALI SEMINARA RENATO	P
DI FONZO FRANCESCO	P	CAVALLARO GIUSEPPE	P
FERRO BRUNO	P	ILARDO PIETRO GIUSEPPE	P
DOTTI CLAUDIO	P	AUREGGI GIULIO LUIGI	P
VECCHIO GIOVANNI	**A**	NITTI FABIO	P
ZANELLA SILVIO	P	TORRE ALBERTO	P
VILLANI RAFFAELE	P	**AGNELLI LUCA**	**A**
DE GASPARI EZIO	P	BASILE RONNIE	P
BOTTASINI GIUSEPPE	P		

Totale presenti 26
Totale assenti 5

Partecipa all'adunanza il **Segretario Generale Dott. Mario Tarricone** il quale provvede alla redazione del presente verbale.
Essendo legale il numero degli intervenuti, il Sig. **Michele Campanale** assume la presidenza e dichiara aperta la seduta per la trattazione dell'argomento indicato in oggetto.

Sono presenti gli assessori signori: Berardi Rosario, Finazzi Walter, Concas Antonio, Mazzeo Francesco
Assistono gli scrutatori signori: Ilardo Pietro, Di Fonzo Francesco, Dotti Claudio .

Discussione: Omissis…per la stessa si fa riferimento al processo verbale ricavato dal nastro magnetico inciso durante il dibattito.

IL CONSIGLIO COMUNALE

PREMESSO:

- Che a seguito dell'emanazione del D. Lgs. 196/2003, "Codice sulla tutela dei dati personali" l'Amministrazione ha adottato con propria delibera consiliare in data 12 maggio 2004 apposito Regolamento comunale per la tutela dei dati personali;
- Che il detto Regolamento necessita di essere integrato nella tabella allegata per quanto concerne i dati trattati dall'Ente e, nella fase di redazione del medesimo, per puro errore, era stato omesso il dovuto riferimento al trattamento dei dati giudiziari;
- Che la bozza di Regolamento, così riformata è stata portata all'esame della Commissione consiliare "Bilancio ed Affari Istituzionali" nella seduta del 19 settembre 2005;
- Che la medesima bozza è stata discussa ed approvata in tale sede;

VISTO quanto disposto dal D. Lgs. 196/2003 in merito alla speciale procedura cui sono sottoposti i Regolamenti comunali sulla riservatezza dei dati personali;

Visto il parere favorevole espresso ai sensi e per gli effetti dell'art. 49 del D. Lgs. 267/2000 in merito alla regolarità tecnica dal Dirigente del Settore Affari Generali in data 19.10.2005;

Vista la dichiarazione del Dirigente del Settore Contabile Finanziario in data 19.9.2005, dalla quale risulta che l'atto non necessita di parere contabile;

Si assentano i Consiglieri Nitti Fabio, Basile Ronnie, Torre Alberto, per cui i presenti risultano essere 23.

Con voti unanimi espressi in modo palese

DELIBERA

DELIBERA

1. di approvare l'integrazione all'art.8 e della Tabella allegata "A" del Regolamento per il trattamento dei dati personali, nel testo che viene allegato alla presente deliberazione;
2. di demandare al Dirigente del Settore Affari Generali gli incombenti relativi alla trasmissione della presente deliberazione al Garante per la protezione dei dati personali.

Rientrano i Consiglieri Nitti Fabio, Basile Ronnie, Torre Alberto, per cui i presenti risultano essere 23.

Letto approvato e sottoscritto:

IL PRESIDENTE
F.to Michele Campanale

IL SEGRETARIO GENERALE
F.to Dott. Mario Tarricone

CERTIFICATO DI ESECUTIVITA'

Si certifica che la suestesa deliberazione:

- è stata pubblicata nelle forme di legge all'Albo Pretorio del Comune, ove rimarrà esposto per quindici giorni consecutivi dal **24/10/2005** art. 124 D.Lgs. n.267 del 18.8.2000).
-

E' DIVENUTA ESECUTIVA IN DATA: 04/11/2005

[X] – ai sensi dell'art.134 comma 3 del D.Lgs. n.267 del 18.8.2000

IL SEGRETARIO GENERALE
F.to Dr. Mario Tarricone

Copia conforme all'originale in carta libera per uso amministrativo

Addì_____

COMUNE DI PIOLTELLO
PROVINCIA DI MILANO

Codice ente 11063	Protocollo n.
DELIBERAZIONE N. **70** DEL **28/11/2005** Trasmessa al C.R.C. [ ]	

VERBALE DI DELIBERAZIONE DEL CONSIGLIO COMUNALE

OGGETTO: **MODIFICHE AL REGOLAMENTO COMUNALE PER LA TUTELA E IL TRATTAMENTO DEI DATI PERSONALI.**

L'anno **duemilacinque** addì **ventotto** del mese di **Novembre**, alle ore **21:00**, nella sala delle adunanze, previa osservanza di tutte le formalità prescritte dalla vigente legge, vennero oggi convocati a seduta i componenti il Consiglio Comunale.

All'appello risultano:

DE GASPARI MARIO	P	DI MONTE LUCIA	P
LEPORE ANTONIO	P	COLOPI MAURO	A
PIETROPAOLO GIUSEPPE	P	BINI GERARDO	A
GERVASI COSIMO	P	GHIRINGHELLI PAOLA	P
FAZIO FRANCESCO	P	CAPUSSELA FABIO	A
GAIOTTO SAIMON	P	COSTANTINO DOMENICO	P
NOVELLI ROSALIA	P	DE CARO STEFANO	A
DI FONZO FRANCESCO	P	ALI SEMINARA RENATO	P
FERRO BRUNO	P	CAVALLARO GIUSEPPE	A
GRAFFEO PASQUALE	P	ILARDO PIETRO GIUSEPPE	P
DOTTI CLAUDIO	P	AUREGGI GIULIO LUIGI	P
VECCHIO GIOVANNI	P	NITTI FABIO	A
ZANELLA SILVIO	P	TORRE ALBERTO	A
VILLANI RAFFAELE	P	AGNELLI LUCA	A
DE GASPARI EZIO	P	BASILE RONNIE	A
BOTTASINI GIUSEPPE	P		

Totale presenti 22
Totale assenti 9

Partecipa all'adunanza il **Segretario Generale Dott. Mario Tarricone** il quale provvede alla redazione del presente verbale. Essendo legale il numero degli intervenuti, il Sig. **Saimon Gaiotto** assume la presidenza e dichiara aperta la seduta per la trattazione dell'argomento indicato in oggetto.

Sono presenti gli Assessori sigg.: Biolchini Roberto, Berardi Rosario, Finazzi Walter, Concas Antonio, Taetti Alberto, Mazzeo Francesco.

Assistono gli scrutatori sigg.: Novelli Rosalia, Dotti Claudio, Ali Seminara Renato.

Discussione:
OMISSIS……per la stessa si fa riferimento al processo verbale ricavato dal nastro magnetico inciso durante il dibattito.

IL CONSIGLIO COMUNALE

PREMESSO:

- Che a seguito dell'emanazione del D. Lgs. 196/2003, "Codice sulla tutela dei dati personali" questa amministrazione si è dotata in data 12 maggio 2004 di apposito Regolamento comunale per la tutela dei dati personali;
- Che detto Regolamento è stato emendato in data 18 ottobre 2005 in quanto per puro errore nella stesura dello stesso, erano state omesse sia nella rubrica dell'articolo sia nell'ultima frase del medesimo le parole "e giudiziari" dopo le parole "..dati sensibili";
- Che l'ANCI con il placet del Garante per la tutela dei dati personali ha emanato degli schemi di Regolamento per i trattamento dei dati sensibili e giudiziari, tra gli altri , per gli EE.LL. che non prevedono in caso di sua adozione necessità di ulteriore parere da parte del Garante;
- Che l'articolato è stato delibato informalmente dal Garante per la parte non ricompressa nello schema di cui sopra e che lo stesso chiede delle modifiche al fine della sua approvazione
- Che l'adeguamento del Regolamento comunale allo schema rilasciato dall'ANCI con il placet del Garante, nonché per la parte ulteriore come sopra specificata, comporta per l'Ente un indiscutibile vantaggio, in quanto lo stesso da un lato non è più da sottoporre al controllo formale, preventivo e vincolante, da parte del Garante stesso per il trattamento dei dati sensibili e giudiziari, mentre per la parte generale con le modifiche richieste, nulla osterà all'approvazione;
- Che la bozza del Regolamento nel nuovo testo è stata portata all'esame della Commissione consiliare "Bilancio ed Affari Istituzionali";
- Che la medesima bozza è stata discussa ed emendata in tale sede;

VISTO:
- Il parere favorevole espresso ai sensi e per gli effetti dell'art. 49 del D. Lgs. 267/2000 in merito alla regolarità tecnica dal Dirigente del Settore Affari Generali, in data 28.11.2005;

VISTA:
- la dichiarazione rilasciata dal Dirigente del Settore Contabilità e Programmazione Finanziaria in data 28.11.2005, dalla quale risulta che il presente provvedimento non necessita di parere di regolarità contabile;

VISTO:
- Quanto disposto dal D. Lgs. 196/2003 in merito alla speciale procedura cui sono sottoposti i Regolamenti comunali sulla riservatezza dei dati personali;

RILEVATO
Che il presente provvedimento non comporta impegno di spesa e non ha pertanto rilevanza sotto il profilo contabile;

Con voti unanimi espressi in modo palese;

DELIBERA

1. di modificare il Regolamento per la tutela e il trattamento dei dati personali come risultante dall'elaborato allegato alla presente deliberazione e di cui fa parte integrante e sostanziale.

2. di demandare ogni atto connesso e consequenziale alla presente deliberazione al Dirigente del Settore Affari Generali.

Letto approvato e sottoscritto:

IL PRESIDENTE
F.to Saimon Gaiotto

IL SEGRETARIO GENERALE
F.to Dott. Mario Tarricone

CERTIFICATO DI ESECUTIVITA'

Si certifica che la suestesa deliberazione:

- è stata pubblicata nelle forme di legge all'Albo Pretorio del Comune, ove rimarrà esposto per quindici giorni consecutivi dal **05/12/2005** art. 124 D.Lgs. n.267 del 18.8.2000).
-

E' DIVENUTA ESECUTIVA IN DATA: 16/12/2005

[X] – ai sensi dell'art.134 comma 3 del D.Lgs. n.267 del 18.8.2000

IL SEGRETARIO GENERALE
F.to Dr. Mario Tarricone

Copia conforme all'originale in carta libera per uso amministrativo

Addì_____

COMUNE DI PIOLTELLO
PROVINCIA DI MILANO

Codice ente 11063	Protocollo n.
DELIBERAZIONE N. 33 DEL 04/04/2006	

VERBALE DI DELIBERAZIONE DEL CONSIGLIO COMUNALE

OGGETTO: **INTEGRAZIONE ALLE TABELLE PER L'UTILIZZO DEI DATI SENSIBILI E GIUIZIARI, ALLEGATI AL REGOLAMENTO COMUNALE PER IL TRATTAMENTO E LA TUTELA DEI DATI PERSONALI**

L'anno **duemilasei** addì **quattro** del mese di **Aprile**, alle ore **21:00**, nella sala delle adunanze, previa osservanza di tutte le formalità prescritte dalla vigente legge, vennero oggi convocati a seduta i componenti il Consiglio Comunale.
All'appello risultano:

DE GASPARI MARIO	**A**	DI MONTE LUCIA	P
LEPORE ANTONIO	P	**COLOPI MAURO**	**A**
PIETROPAOLO GIUSEPPE	P	BINI GERARDO	P
GERVASI COSIMO	P	GHIRINGHELLI PAOLA	P
FAZIO FRANCESCO	P	**CAPUSSELA FABIO**	**A**
GAIOTTO SAIMON	P	COSTANTINO DOMENICO	P
NOVELLI ROSALIA	P	DE CARO STEFANO	P
DI FONZO FRANCESCO	P	ALI SEMINARA RENATO	P
FERRO BRUNO	P	CAVALLARO GIUSEPPE	P
GRAFFEO PASQUALE	P	ILARDO PIETRO GIUSEPPE	P
DOTTI CLAUDIO	P	AUREGGI GIULIO LUIGI	P
VECCHIO GIOVANNI	**A**	**NITTI FABIO**	**A**
ZANELLA SILVIO	P	**TORRE ALBERTO**	**A**
VILLANI RAFFAELE	P	**AGNELLI LUCA**	**A**
DE GASPARI EZIO	P	**BASILE RONNIE**	**A**
BOTTASINI GIUSEPPE	P		

Totale presenti 23
Totale assenti 8

Partecipa all'adunanza il **Segretario Generale Dott. Mario Tarricone** il quale provvede alla redazione del presente verbale.
Essendo legale il numero degli intervenuti, il Sig. **Saimon Gaiotto** assume la presidenza e dichiara aperta la seduta per la trattazione dell'argomento indicato in oggetto.

Sono presenti gli assessori signori: Concas Antonio, Mazzeo Francesco

Assistono gli scrutatori signori, Di Monte Lucia, Ferro Bruno, Aureggi Giulio

Discussione: Omissis…per la stessa si fa riferimento al processo verbale ricavato dal nastro magnetico inciso durante il dibattito.

Il CONSIGLIO COMUNALE

PREMESSO:

- Che a seguito dell'emanazione del D. Lgs. 196/2003, "Codice sulla tutela dei dati personali" questa amministrazione si è dotata di apposito Regolamento comunale per la tutela dei dati personali, in seguito due volte emendato e integrato;
- Che detto Regolamento, redatto secondo le indicazioni del Garante, presenta delle lacune in quanto non ricomprende dei trattamenti di dati sensibili che necessitano invece di essere trattati dall'Ente per l'assolvimento dei compiti istituzionali assegnati, nonché per essere adeguato catalizzatore della crescita culturale della cittadinanza;
- Che il Garante ha rilasciato parere che prevede l'integrazione dei regolamenti comunali con quelle attività che risultavano escluse dal trattamento;
- L'adeguamento del Regolamento comunale, in assenza di direttive diverse da parte del Garante, esattamente si conforma agli schemi in precedenza approvati da garante stesso;
- Che la bozza delle integrazioni è stata portata all'esame della Commissione consiliare "Bilancio ed Affari Istituzionali" nella seduta del 27-03-2006**;**
- Che la medesima bozza è stata discussa ed approvata in tale sede;
- Che il presente provvedimento non comporta impegno di spesa e non ha pertanto rilevanza sotto il profilo contabile;

VISTO:
- Il parere favorevole espresso ai sensi e per gli effetti dell'art. 49 del D. Lgs. 267/2000 in merito alla regolarità tecnica dal Dirigente del Settore Affari Generali in data 29.3.2006;
-
Vista la dichiarazione del Dirigente del Settore Contabilità e Programmazione Finanziaria in data 30.3.2006, dalla quale risulta che l'atto non necessita di parere contabile;

Con voti unanimi espressi in modo palese

DELIBERA

1. di modificare ed integrare la tabella 20 esistente, sostituendola come nell'allegato, e di inserire le nuove tabelle 36 e 37 anch'esse in allegato.

2. di demandare ogni atto connesso e consequenziale alla presente deliberazione al Dirigente del Settore Affari Generali.

Entrano gli assessori Taetti Alberto, Berardi Rosario.

Letto approvato e sottoscritto:

IL PRESIDENTE
F.to Saimon Gaiotto

IL SEGRETARIO GENERALE
F.to Dott. Mario Tarricone

CERTIFICATO DI ESECUTIVITA'

Si certifica che la suestesa deliberazione:

- è stata pubblicata nelle forme di legge all'Albo Pretorio del Comune, ove rimarrà esposto per quindici giorni consecutivi dal **06/04/2006** art. 124 D.Lgs. n.267 del 18.8.2000).
-

E' DIVENUTA ESECUTIVA IN DATA: 17/04/2006

[X] – ai sensi dell'art.134 comma 3 del D.Lgs. n.267 del 18.8.2000

IL SEGRETARIO GENERALE
F.to Dr. Mario Tarricone

Copia conforme all'originale in carta libera per uso amministrativo

Addì_____