COMUNE DI BAGNACAVALLO

Provincia di Ravenna

DELIBERAZIONE DELLA **GIUNTA COMUNALE N. 211** DEL **29/12/2005**

OGGETTO: REGOLAMENTO SULLE MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI.

L'anno 2005 addì ventinove del mese di Dicembre alle ore 12:00 in Bagnacavallo nel Palazzo Comunale.

Previa l'osservazione di tutte le formalità prescritte dalla vigente legge comunale e provinciale, si sono oggi riuniti i componenti la Giunta Comunale, Signori:

		Presente
ROSSI LAURA	*Sindaco*	S
RAVAGLI PIERLUIGI	*Vice Sindaco*	S
BALLARDINI RAFFAELLA	*Assessore*	S
BETTI LUCIA	*Assessore*	S
BIANCHI LISA	*Assessore*	S
GOLFIERI CARLA	*Assessore*	S
GRAZIANI PAOLO	*Assessore*	S
PRONI ELEONORA	*Assessore*	S

Constatata la legalità del numero dei presenti, assume la presidenza
il Sig. ROSSI LAURA *Sindaco*

Partecipa il Dott. DELLACASA BELLINGEGNI ANNA MARIA Segretario.

ANNOTAZIONI
Pubblicata col. Prot.
N. 17 del 09.02.2006

LA GIUNTA COMUNALE

vista la normativa in materia di trattamento dei dati personali e, in particolare, il "Codice in materia di protezione dei dati personali" approvato con il d. lgs. 196/03;

considerato che tale normativa è improntata al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Ogni trattamento dei dati personali, infatti, deve svolgersi in conformità al principio di necessità nel trattamento dei dati, in base al quale i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi o altre modalità che permettano di identificare l'interessato solo in caso di necessità.

dato atto che:
- la sicurezza dei dati personali è oggetto di regolamentazione in via generale e il Consiglio Comunale di Bagnacavallo ha adottato, con deliberazione n. 84 del 22.12.2005, il regolamento per il trattamento dei dati sensibili e giudiziari redatto ai sensi del "Codice in materia di protezione dei dati personali";
- il Sindaco ha nominato i "responsabili dei trattamenti", i quali possono delegare alcune funzioni agli "incaricati dei trattamenti";
- i responsabili/incaricati dei trattamenti hanno effettuato il censimento delle banche-dati gestite dalle varie strutture, facendo riferimento ad un concetto ampio della nozione di banca-dati, comprendente sia gli archivi informatizzati (hard disk, floppy-disk, CD rom, memorie di rete, ecc.) sia gli archivi cartacei, tutti da sottoporre a idonee misure di sicurezza;

ritenuto di dover individuare adeguate misure di sicurezza, in conformità alle linee d'indirizzo definite dal Consiglio Comunale n sede regolamentare;

vista la proposta redatta dal "Responsabile dei sistemi informativi automatizzati" (d. lgs. 39/93), che prende in considerazione i principali profili di rischio (distruzione o perdita di dati, accesso non autorizzato o trattamento non consentito), disponendo idonee misure di cautela:

dato atto della regolarità tecnico-amministrativa della presente determinazione;

accertato il parere favorevole di regolarità contabile e l'attestazione relativa alla copertura finanziaria espresso del responsabile del servizio finanziario ai sensi e per gli effetti dell'art. 51 comma 4 del d.lgs. 18.8.2000, n. 267;

con voti favorevoli unanimi;

DELIBERA

1) Di approvare il documento allegato quale parte sostanziale e integrante della presente deliberazione, contenente:
a) le "Misure minime di sicurezza" (di cui al Disciplinare tecnico in materia di misure minime di sicurezza, allegato B del Codice in materia di protezione dei dati personali) finalizzate alla tutela della riservatezza dei dati personali, in relazione alla generalità dei trattamenti effettuati dal Comune;

b) il "Documento programmatico sulla sicurezza" (di cui al punto 19 del citato allegato B del Codice in materia di protezione dei dati personali) con particolare riferimento ai trattamenti elettronici di dati sensibili o giudiziari

c) il censimento delle banche dati rilevate nel Comune alla data odierna.

Misure minime di sicurezza

Il presente documento contiene le misure minime di sicurezza finalizzate alla tutela della riservatezza dei dati personali, in relazione ai trattamenti effettuati nel Comune compresi nel censimento delle banche dati di seguito elencate.

Banche dati trattate senza l'ausilio di strumenti elettronici:

- Archivio corrente
- Archivio di deposito
- Documentazione in carico agli uffici
- Atti depositati presso il messo notificatore

Banche dati trattate con l'ausilio di strumenti elettronici:

Installate in elaboratori non in rete:
- Polizia Municipale
- Stato Civile
- Controllo delle presenze
- Traffico telefonico
- Utenti dei servizi sociali a retta
- Anagrafe canina
- Risultati elettorali
- Inventario dei beni immobili
- Albo delle associazioni
- Opere pubbliche

Installate in elaboratori in rete:
- Personale dipendente ed amministratori
- Fornitori
- Anagrafe e Leva
- Concessioni edilizie
- Protocollo
- Deliberazioni e Segreteria
- Contabilità
- Tributi

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

RISCHIO: Intrusione di soggetti estranei nell'ufficio.

MISURE DI SICUREZZA
- Impianto di allarme o vigilanza notturna
- Chiusura degli edifici con chiave in dotazione ad ogni addetto
- Verbale di consegna delle chiavi alla ditta delle pulizie

(v. anche normativa specifica sulla custodia delle carte d'identità)

RISCHIO: Intrusione di soggetti non autorizzati in armadi e cassetti

MISURE DI SICUREZZA
- Chiusura di armadi e cassetti con chiave in dotazione ai soli soggetti incaricati di trattare i dati
- Nomina scritta da parte del "responsabile del trattamento" dei soggetti "incaricati" autorizzati al trattamento dei dati personali (con aggiornamento espresso del relativo elenco ad ogni variazione)
- Identificazione di tutti coloro che accedono ad archivi contenenti dati sensibili
- Divieto di conservare documenti contenenti dati sensibili fuori dagli armadi e dai cassetti (salvo chiusura a chiave dell'ufficio)
- Diffusione di istruzioni sull'adozione delle necessarie cautele in materia
- Controlli e sanzioni per le principali inadempienze

RISCHIO: Diffusione di documenti contenenti dati personali non conforme all'ordinamento

MISURE DI SICUREZZA
- Diffusione di istruzioni sull'adozione delle necessarie cautele in materia
- Controlli e sanzioni per le principali inadempienze
- Idonee cautele nell'ambito delle convenzioni con i soggetti esterni (comuni, provincia, ministeri, aziende di outsourcing e concessionari di pubblico servizio, ecc.), autorizzati ad accedere in modo controllato ai dati personali. In particolare, occorre inserire nei capitolati d'oneri clausole specifiche che assicurino la legittimità dei trattamenti, che in ogni caso devono essere pertinenti alla gestione del servizio.

RISCHIO: Incendi o allagamenti (perdita di dati)

MISURE DI SICUREZZA
- Locali archivio conformi alle prescrizioni dettate in materia (controllo temperatura, umidità, luce ecc.)
- Rispetto del divieto di fumo
- Rispetto adempimenti del d.lgs. 626
- Adempimenti prescritti dai VV.d.FF.

TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

RISCHIO: Danni ai programmi e/o perdita dei dati (virus, sbalzi di corrente, eventi atmosferici ecc.)

MISURE DI SICUREZZA
- archiviazione dei dati sul server, con salvataggio automatico giornaliero
- conservazione dati back up in contenitori ad isolamento termico e magnetico, in luogo accessibile solo al personale autorizzato
- modalità di ripristino dei dati in caso di danneggiamento: utilizzo dati back up (nel minor tempo possibile e comunque entro il termine massimo di 7 giorni dalla scoperta del danno)
- divieto di istallare programmi, salvaschermi, ecc. senza previa autorizzazione dell'amministratore di sistema
- divieto di accesso a Internet per esigenze non legate a compiti di ufficio (le violazioni sono sanzionate sul piano disciplinare e/o penale)
- divieto di aprire allegati di e-mail che lascino sospettare virus, senza prima aver contattato l'amministratore di sistema per un controllo
- verifica periodica sull'affidabilità dei sistemi di elaborazione dati, dei sistemi operativi e delle applicazioni software
- obbligo di aggiornamento dei dispositivi antivirus con cadenza almeno mensile, ove possibile in automatico

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da virus informatici l'Amministratore di sistema, su eventuale segnalazione del responsabile del trattamento, deve provvedere a:
- Isolare il sistema
- Verificare se ci sono altri sistemi infettati con lo stesso virus informatico
- Identificare l'antivirus adatto e bonificare il sistema infetto
- Installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

A.5: CUSTODIA E CONSERVAZIONE DEI SUPPORTI UTILIZZATI PER IL BACK-UP DEI DATI

L'Amministratore di sistema è responsabile della custodia e della conservazione di supporti utilizzati per il back-up dei dati. Il back up viene effettuato con modalità differenziate e in luoghi distinti, a tutela di eventuali imprevisti quali furto, incendio, ecc.

Per ogni banca dati deve essere indicato il luogo di conservazione ed i supporti utilizzati per il back-up dei dati.

L'accesso ai supporti utilizzati per il back-up dei dati è limitato per ogni banca di dati ai seguenti soggetti:
- Responsabile della sicurezza dei dati
- Eventuale Responsabile del trattamento di competenza
- Incaricato del trattamento di competenza
- Amministratore di sistema di competenza

A.6: UTILIZZO E RIUTILIZZO DEI SUPPORTI MAGNETICI

In relazione ai supporti magnetici utilizzati per le copie di back-up delle banche di dati trattate non più utilizzati per gli scopi per i quali erano stati destinati, deve provvedersi a cancellare il contenuto annullando e rendendo illeggibili le informazioni in esso contenute.

E' fondamentale che il Responsabile del trattamento dei dati, con il supporto tecnico dell'Amministratore di sistema, si assicuri che in nessun caso vengano lasciate copie di back-up delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.

Rischio B: ACCESSO NON AUTORIZZATO E/O TRATTAMENTO NON CONSENTITO

Misure da adottare

B.1: NORME GENERALI DI PREVENZIONE

Per far fronte al rischio di un accesso non autorizzato e/o di un trattamento non consentito, in relazione soprattutto ai files contenenti dati sensibili, occorre attenersi alle seguenti prescrizioni: accesso controllato ai dati personali; distruzione immediata dei dati non pertinenti e cancellazione dei dati dopo il definitivo utilizzo.

E' opportuno inoltre formalizzare il divieto di:
- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile del trattamento di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento dei dati, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.

- Consegnare a persone non autorizzate dal Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

B.2: PROCEDURE PER CONTROLLARE L'ACCESSO AI LOCALI IN CUI VENGONO TRATTATI I DATI

Al Responsabile del trattamento dei dati, eventualmente con il supporto tecnico dell'Amministratore di sistema, è affidato il compito di redigere a di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati per controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il Responsabile del trattamento dei dati, eventualmente con il supporto tecnico dell'Amministratore di sistema, deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

B.3: CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA DELLE TRASMISSIONI DEI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il Responsabile del trattamento dei dati, eventualmente con il supporto tecnico dell'Amministratore di sistema, stabilisce le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.

I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- Le misure applicate per evitare intrusioni quali l'adozione consigliata di sistemi di firewall e la registrazione degli accessi tramite file di log;
- Le misure applicate per evitare contagi da virus informatici con l'installazione di adeguati software "vaccino" e "curativi".

B.4: GESTIONE ELETTRONICA DEI DATI PERSONALI ATTI A RIVELARE LO STATO DI SALUTE E LA VITA SESSUALE

La soluzione tecnologica che sarà adottata nella gestione di tale categoria di dati sarà compatibile con il codice della privacy. La cifratura dei dati o la separazione dei dati identificativi da quelli sensibili riguarda solo gli organismi sanitari e gli esercenti professioni sanitarie (regola 24).

B.5: GESTIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Responsabile del trattamento dei dati, con il supporto tecnico dell'Amministratore di sistema, è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli Incaricati autorizzati al trattamento dei dati personali così come le configurazioni di accesso ai programmi e ai dati informatici correlati alle funzionalità associate agli Incaricati *(v. periodico rilascio di password legate allo Schema organizzativo generale).*

E' inoltre consigliabile redigere la tabella dei Permessi di accesso, che indica per ogni banca di dati i tipi di permesso di accesso per ogni Incaricato del trattamento autorizzato. In particolare è auspicabile per ogni Incaricato del trattamento e per ogni banca di dati indicare i privilegi assegnati tra i seguenti:

- Inserimento di dati
- Lettura e stampa di dati
- Variazione di dati
- Cancellazione di dati

B.6: VERIFICHE PERIODICHE DELLE CONDIZIONI PER IL MANTENIMENTO

DELLE AUTORIZZAZIONI

Ai Responsabili del trattamento dei dati, eventualmente con il supporto tecnico dell'Amministratore di sistema, è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare – se necessario - l'elenco degli utenti autorizzati

---

PIANO DI RIPRISTINO IN CASO DI DISTRUZIONE O DANNEGGIAMENTO DEI DATI O DEGLI STRUMENTI ELETTRONICI

Sono attive procedure di back-up dei dati in computer ubicati presso edifici sufficientemente distanti per cui eventi quali incendi, furti, crolli e guasti hardware sono affrontabili con procedure di ripristino dei servizi nei tempi prescritti dall'ordinamento.

PIANO DI FORMAZIONE DEGLI INCARICATI

Al Responsabile del trattamento dei dati, con il supporto tecnico dell'Amministratore di sistema e sotto la sovrintendenza della direzione generale, è affidato il compito di verificare ogni anno, entro il 31 Dicembre, le necessità di formazione del personale incaricato dei vari adempimenti.

TRATTAMENTI DI DATI PERSONALI AFFIDATI ALL'ESTERNO DELLA STRUTTURA

E' possibile affidare la gestione di dati a soggetti esterni alla struttura dotati dei necessari requisiti di idoneità, nei limiti previsti dall'ordinamento, fermo restando che tale affidamento deve essere pertinente all'esercizio di un determinato servizio pubblico. In particolare, occorre delimitare la trasmissione di dati sensibili alla casistica strettamente indispensabile per lo svolgimento del servizio.

Si fa rinvio in proposito al contenuto delle "misure minime", sopra riportato, da applicare in relazione ai dati sensibili con un più rafforzato livello di tutela.

REVISIONE PERIODICA DELLE MISURE DI SICUREZZA

I responsabili del trattamento dei dati, con il supporto tecnico dell'Amministratore di sistema, assumono l'impegno di procedere ad una revisione periodica del presente documento (almeno annualmente) e di predisporre le modifiche/integrazioni eventualmente necessarie.

Letto, confermato e sottoscritto

IL SINDACO
F.to ROSSI LAURA

IL SEGRETARIO COMUNALE
F.to DELLACASA BELLINGEGNI ANNA MARIA

CERTIFICATO DI PUBBLICAZIONE

Del presente atto deliberativo viene iniziata oggi la pubblicazione all'Albo Pretorio per quindici giorni consecutivi.

Dalla Residenza Municipale, addì 08 FEB. 2006

IL SEGRETARIO COMUNALE
DELLACASA BELLINGEGNI ANNA MARIA

CERTIFICATO DI ESECUTIVITA'

☐ **E' dichiarata immediatamente eseguibile (Art. 134 D. Lgs. 267/2000)**

Esecutiva il giorno 20 FEB. 2006 **ai sensi 3° comma dell'art. 134 D.lgs 267/2000**

Bagnacavallo, _____

IL SEGRETARIO COMUNALE
DELLACASA BELLINGEGNI ANNA MARIA

Copia conforme per uso amministrativo.

Lì, _____

IL SEGRETARIO COMUNALE