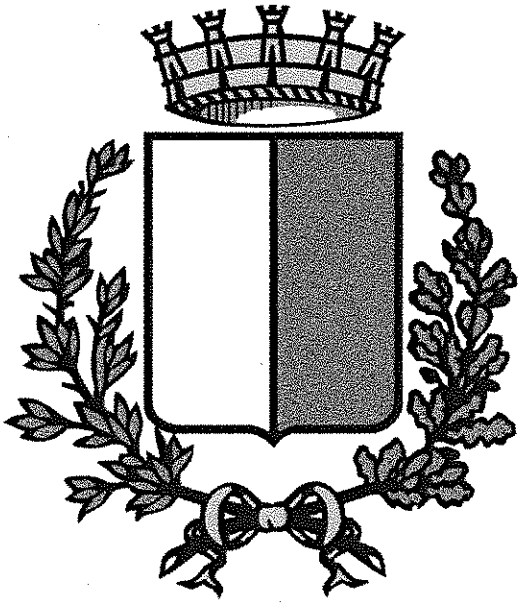

COMUNE DI BARI

DISPOSIZIONI IN MATERIA DI
PROTEZIONE DEI "DATI PERSONALI"
(ex D.Lgs. n.196/2003)

Approvato con delibera di G.M. n. **849** del **3/12/2015**

INDICE

3. – AGGIORNAMENTO, REVISIONE, PUBBLICITÀ ED ENTRATA IN VIGORE

INTRODUZIONE

Le presenti Disposizioni sulla Privacy intendono essere uno strumento di applicazione del Decreto Legislativo 30 giugno 2003, n. 196 (il cosiddetto "Codice sulla privacy") nell'ambito dell'organizzazione Comunale e parte da un'attenta analisi delle problematiche concrete che quotidianamente emergono nella tutela della riservatezza dei dati personali in ambito istituzionale. La redazione di un Documento aziendale sulla Privacy si è resa necessaria dopo l'entrata in vigore del Codice, che non solo riordina l'intera normativa in tema di trattamento di dati personali, riunendo in un unico contesto la Legge 31 dicembre 1996, n. 675 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi ultimi anni, ma apporta anche numerose integrazioni e modificazioni, tenendo conto della "giurisprudenza" del Garante per la protezione dei dati personali e della direttiva dell'Unione Europea 2000/58 sulla riservatezza nelle comunicazioni elettroniche. Nell'opera di sistemazione dell'intera disciplina il legislatore si è ispirato ai principi di semplificazione ed efficacia, integrando e approfondendo numerosi aspetti che riguardano il trattamento dei dati personali da parte della Pubblica Amministrazione. Il documento "Disposizioni in materia di protezione dei dati e Disciplinare interno sull'utilizzo della documentazione cartacea e della dotazione informatica" è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante. Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della Privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle PP.AA., di una riservatezza totale dal punto di vista reale e sostanziale.

Il diritto alla riservatezza è un vero e proprio diritto inviolabile della persona che non si limita alla tutela e protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità. Per questi motivi la cultura della Privacy necessita di crescere e rafforzarsi perché solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di legge, nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con il Cittadino.

1. DISPOSIZIONI

PREMESSA

In ottemperanza alle disposizioni del ***Codice in materia di protezione dei dati personali*** (D.Lgs n. 196/03) per i dipendenti del Comune di Bari, ed in relazione alle attività svolte nell'ambito della Strutture di appartenenza, il trattamento di *dati personali* da essi posto in essere dovrà essere effettuato attenendosi alle seguenti istruzioni ed ad ogni ulteriore indicazione, anche verbale in via eccezionale, che potrà essere fornita dal *Titolare*[1] o dai competenti *Responsabili*[2] del trattamento in parola.

I "***dati personali***" devono essere trattati:

- in osservanza dei criteri di riservatezza;
- in modo lecito e secondo correttezza;
- per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Si precisa che, a seguito Decreto Semplificazioni ex D.L. 9-02-2012 n.5, non vi è più l'obbligo di redigere il DPS (documento programmatico sulla sicurezza) entro il 31 Marzo di ogni anno. Tuttavia rimangono invariate tutte le altre misure minime di sicurezza fisica, logica ed organizzativa imposte dalla normativa vigente.

Le "***misure minime di sicurezza***"[3] definite per il *trattamento dei Dati Personali* del Comune di Bari, sono obbligatorie e distinte in funzione delle seguenti modalità di trattamento:

a) senza l'ausilio di strumenti elettronici (ossia mediante **documentazione cartacea**);

b) con l'ausilio di strumenti elettronici (ossia mediante **dotazione informatica**).

---

1 VEDI DEFINIZIONE: art. 4, comma 1 – sub. f) del *Codice in materia di protezione dei dati personali* (D.Lgs. n. 196/03).

2 VEDI DEFINIZIONE: art. 4, comma 1 – sub. g) del *Codice in materia di protezione dei dati personali* (D.Lgs. n. 196/03).

3 Vedi artt. 33–36 del DLgs.196/03 ed annesso ALL. B *"Disciplinare Tecnico in Materia di Misure Minime di Sicurezza"."*

Art. 1.1 – OGGETTO.

1. Il presente Documento, in attuazione del "*Codice in materia di protezione dei dati personali*", approvato con **D.Lgs. 30 giugno 2003, n.196** (di seguito "***Codice Privacy***") intende disciplinare:

a) il *trattamento dei Dati Personali* contenuti nelle banche dati organizzate, gestite o utilizzate dal Comune di Bari;

b) l'individuazione e le competenze del **"Titolare"**, dei **"Responsabili"**, degli **"Incaricati"**[4] del loro trattamento e dell' **"Amministratore di Sistema"** (***AdS***);

c) le modalità di adempimento agli obblighi in materia di "misure di sicurezza", al fine di garantire il corretto trattamento cartaceo e/o informatizzato dei dati.

Art. 1.2 – DEFINIZIONI

1. Ai fini del presente Documento, per le restanti definizioni di:

banca dati, trattamento, , dati sensibili, dati giudiziari, interessato, comunicazione, diffusione, dato anonimo, blocco e Garante, nonché per i contenuti delle attività di trattamento, si fa riferimento a quanto previsto dalla normativa vigente in materia[5].

2. Per *finalità istituzionali* si intendono:
- le funzioni previste dalla legge, dallo Statuto e dai Regolamenti del Comune di Bari;
- le funzioni svolte per mezzo di accordi, intese e mediante gli strumenti di programmazione negoziata previsti dalla legislazione vigente;
- i compiti e le attività svolte in relazione ai programmi esplicitati nella Relazione Previsionale e Programmatica ed i relativi obiettivi recepiti nel Piano Esecutivo di Gestione;
- i compiti e le attività che risultino comunque necessari per lo svolgimento delle funzioni indicate nei punti precedenti.

Art. 1.3 – PRINCIPI GENERALI

1. Il Comune di Bari effettua il *trattamento dei Dati Personali* conformandosi ai principi di semplificazione, armonizzazione ed efficacia[6] sia per le modalità di esercizio dei diritti da parte degli *Interessati*, sia per l'adempimento degli obblighi a cui è soggetto come *Titolare*.

2. Il Sistemi informativo del Comune di Bari ed i programmi informatici di detto Sistema sono configurati riducendo al minimo l'utilizzazione di dati personali, attenendosi al principio di necessità[7] e mediante verifica della pertinenza e non eccedenza dei dati trattati rispetto alle funzioni assolte o ai servizi erogati.

3. L'utilizzo della documentazione cartacea contenente dati personali deve avvenire in base al principio della necessità dell'uso ovvero gli essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni.
Altresì i *dati personali* non devono essere comunicati all'esterno e comunque a soggetti terzi se non previa autorizzazione del *Titolare* o del competente *Responsabile del trattamento* nel rispetto del vigente *Codice Privacy*.

---

4 VEDI DEFINIZIONE: art. 4, comma 1 – sub. h) del *Codice in materia di protezione dei dati personali* (D.Lgs. n. 196/03).

5 VEDI ALTRE DEFINIZIONI: art.4 del "Codice Privacy".

6 Vedi art. 2, comma 2, del "Codice Privacy".

7 Vedi art. 3 del "Codice Privacy".

Art. 1.4 - TITOLARE DEL TRATTAMENTO

1. **TITOLARE** del *trattamento dei Dati Personali* effettuato dal Comune di Bari risulta essere, nell'ambito della propria organizzazione, il **SINDACO PRO TEMPORE** in quanto l'Ente territoriale locale manifesta la propria volontà, nel suo complesso, mediante questi[8].

2. Il Titolare provvede:

a) ad assolvere all'obbligo di notificazione al Garante nei limiti e con le modalità prescritte dalla normativa vigente in materia;

b) a richiedere, ove necessario, le autorizzazioni e ad effettuare le dovute comunicazioni al Garante per il trattamento o la comunicazione dei dati;

c) ad adottare, per quanto di competenza, le misure necessarie a garantire la sicurezza dei dati personali;

d) a nominare i ***Responsabili del Trattamento Dati,*** relativamente ad ogni Ripartizione/POS/Circoscrizione comunale

e) ad impartire per iscritto ai Responsabili le necessarie istruzioni e le direttive di massima per la corretta gestione e tutela dei dati personali, ivi compresa la loro integrità e sicurezza;

f) a verificare periodicamente la corrispondenza dell'attività svolta dai Responsabili alle disposizioni di legge e regolamentari, alle istruzioni ed alle direttive impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

g) agli adempimenti prescritti dal Codice Privacy riguardo all'adozione delle misure minime di sicurezza

Art. 1.5 - RESPONSABILI DEL TRATTAMENTO

1. I *Responsabili del Trattamento dei Dati Personali* sono designati dal *Titolare* tra i Dirigenti dell'Ente. Tenuto conto dell'organizzazione della struttura del Comune di Bari, essi vengono individuati anche a livello di Responsabili di Servizio. Essi sono responsabili di tutte le banche dati utilizzate dagli uffici di rispettiva competenza, nonché dei relativi trattamenti specifici. Per esigenze organizzative il *Titolare* può nominare, con specifico atto, altri *Responsabili del trattamento*, scelti tra i non Dirigenti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza[9].

2. In generale, il *Responsabile del Trattamento dei Dati personali*, attenendosi alle istruzioni impartite dal Titolare:

a) nomina per iscritto, per quanto di competenza, gli ***Incaricati del Trattamento Dati,*** per ciascun tipologia di trattamento presente nella propria struttura, sulla base delle direttive di massima impartite dal Titolare, delle istruzioni pratiche per il corretto *trattamento dei Dati Personali*, specificando l'ambito del trattamento consentito a ciascuno di essi ed eseguendo gli opportuni controlli successivi. Le nomine degli INCARICATI del trattamento dopo la firma per presa visione devono essere conservate nel fascicolo "Protezione Dati Personali" della Struttura. e, ai fini di una eventuale ispezione, devono essere costantemente aggiornate seguendo il flusso del cambiamento del personale (trasferimenti/ e delle attività a ciascuno di essi assegnate.

b) in materia di trattamento di dati sensibili e giudiziari adotta idonee e preventive misure di sicurezza volte a dare piena attuazione alle disposizioni contenute nella vigente normativa, definendo soluzioni tecniche, informatiche, organizzative, logistiche e procedurali che tengano

---

8 Vedi art. 28 del Codice Privacy.

9 Vedi art. 29 del Codice Privacy.

conto della specificità del trattamento dei dati in questione e delle particolarità connesse alle operazioni su di essi eseguibili;

c) cura il coordinamento di tutte le operazioni di trattamento di dati personali affidate alla struttura di propria competenza;

d) provvede, con cadenza almeno annuale, alla verifica ed al censimento delle banche dati esistenti e stabilisce, all'occorrenza, le procedure da adottare per il trattamento di nuovi o particolari categorie di *dati personali* della propria struttura;

e) provvede a che sia assicurata la corretta informativa alla persona fisica, giuridica, ente o associazione cui si riferiscono i dati personali, ovvero alla persona presso la quale i dati stessi sono raccolti;

f) vigila sulla comunicazione dei dati personali e sulla loro diffusione;

*g)*dispone il blocco dei dati, qualora sia necessaria una sospensione temporanea delle operazioni di trattamento.

*h)*provvede, al fine di facilitare operazioni di reperibilità della documentazione necessaria in caso di controlli da parte del Garante, alla creazione di un fascicolo "Protezione dei Dati Personali" della Struttura di propria competenza.

3. Il *Responsabile del Trattamento* ha, altresì, l'obbligo:

a) di verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza e non eccedenza rispetto alle finalità perseguite nei singoli casi disponendone, se necessario, la cancellazione totale o parziale;

b) di non utilizzare i dati che, a seguito delle verifiche eseguite, risultano eccedenti o non pertinenti o non necessari;

c) di trattare i dati sensibili e giudiziari contenuti in elenchi, registri o banche dati, tenuti con l'ausilio di strumenti elettronici, o comunque automatizzati, mediante l'utilizzo di tecniche (ad es. di *crittografia*) che permettono, di identificare gli *Interessati* solo in caso di necessità;

d) di conservare separatamente da ogni altro i dati idonei a rivelare lo stato di salute e la vita sessuale, adottando le cautele di cui alla lettera precedente anche quando sono tenuti in archivi o banche di dati senza l'ausilio di strumenti elettronici.

4. È fatto obbligo al Responsabile di custodire la propria nomina, sottoscritta per accettazione, nel fascicolo "Protezione dei Dati Personali" presente nella struttura diretta e di inviarne copia alla Ripartizione Segreteria Generale Posizione Organizzativa Protezione dei Dati Personali.

Art. 1.6 - INCARICATI DEL TRATTAMENTO

1. I *Responsabili del trattamento* provvedono, nell'ambito delle strutture di competenza, alla nomina individuale dei soggetti incaricati del trattamento mediante specifica ***nomina di incaricato al trattamento.***

2. le nomine di Incaricato, firmate per presa visione, vengono custodita nel fascicolo "Protezione Dati Personali" presente nella struttura di appartenenza devono essere costantemente aggiornate seguendo il flusso del cambiamento del personale (trasferimenti/ e delle attività a ciascuno di essi assegnate.

3. L'***Incaricato***[10] *del TRATTAMENTO DEI DATI PERSONALI* può essere, altresì, individuato attraverso la documentata preposizione della persona fisica ad una Struttura per la quale è stato individuato, per iscritto, l'ambito di trattamento consentito agli addetti dell'unità medesima.

---

10 Come previsto dall'art. 30, comma 2., del Codice Privacy.

4. Gli *Incaricati* effettuano le operazioni di trattamento dei dati conformandosi alle istruzioni del *Titolare e* dei *Responsabili del trattamento*, nel rispetto della normativa vigente e della prassi interna anche per quanto riguarda gli interventi da attuare in materia di sicurezza dei dati e dei sistemi. Provvedono a fornire l'*informativa Privacy*[11] agli *Interessati* e verificano che ciascuna operazione di comunicazione e diffusione dei dati sia conforme alle disposizioni di Legge e del presente Regolamento.

5. Nei casi di **trattamenti occasionali di *Dati Personali*** che siano da svolgere da parte di soggetti esterni (stagisti, tirocinanti etc.), il competente *Responsabile del trattamento* nomina per iscritto, tali soggetti come ***Incaricati al trattamento*** per specifici ambiti e di specifiche operazioni, fornendo loro le necessarie istruzioni operative.

Art. 1.7 – RESPONSABILE DEI SISTEMA INFORMATIVO COMUNALE

1. Il Responsabile del Sistema Informativo Comunale nella figura del Dirigente della Ripartizione Innovazione Tecnologica garantisce e tutela la sicurezza delle reti informatiche e delle banche dati centralizzate nel rispetto dei principi sanciti dal Codice Privacy e collabora con il Titolare, con i Responsabili del trattamento competenti e con l'Amministratore di Sistema per l'individuazione delle soluzioni informatiche più idonee, tenuto conto della specificità dei trattamenti effettuati.

Art. 1.8 – AMMINISTRATORE DI SISTEMA

1. Il Titolare del trattamento ha posto in essere ed adeguato la figura professionale di Amministratore di Sistema, in ossequio sia al primario DPR. 319/99 che, da ultimo al Provvedimento del Garante della Privacy, datato 27 Novembre 2008, recante "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema".
2. L'Amministratore di Sistema in via generale provvede a:

- Rispondere alle esigenze del Responsabile del Servizio di appartenenza;
- Informare tempestivamente il Titolare del Trattamento dei Dati ed il Responsabile del Sistema Informativo Comunale sulle incongruenze rilevate con le norme di sicurezza e su eventuali incidenti, proponendo misure preventive e correttive;
- Impartire agli incaricati, d'intesa con il Responsabile del trattamento dei Dati Personali per quanto attiene gli aspetti organizzativi, istruzioni tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- Gestire il sistema informatico comunale applicando ad esso le misure di sicurezza informatica;
- Monitorare la struttura e gli apparati di rete informatica (LAN-WAN-Wifi) anche in collaborazione con eventuali tecnici esterni all'Amministrazione, sovrintendendo al loro operato, sia per la fornitura di Hw-Sw che negli interventi di manutenzione dei sistemi operativi ed applicativi installati;
- Installare e configurare nuovo hardware/software sia lato client che lato server per intervenuta esigenza di implementazione dei medesimi;
- Gestire il sistema di autenticazione ed autorizzazione per gli accessi degli operatori in rete;
- Rispondere alle esigenze operative degli utenti di rete;
- Pianificare e verificare la corretta esecuzione dei backup dei dati centralizzati;

Applicare le patch correttive e gli aggiornamenti ai software necessari sia lato client che lato server.
3. L'Amministratore di Sistema avrà l'obbligo di rispettare il segreto sulle informazioni e sui dati personali di cui viene, anche accidentalmente, a conoscenza nell'esercizio della propria funzione

---

[11] Vedi successivo *Art. 1.12* e, più in generale, ai sensi dell'art. 13 del Codice Privacy.

(art. 326 codice penale e art. 15 D.P.R. n. 3/1957); tale obbligo permarrà anche dopo la cessazione dell'incarico.
4. L'operato dell'Amministratore di Sistema sarà oggetto di un'attività di verifica da parte del Titolare o del Responsabile del Sistema Informativo, con cadenza almeno annuale in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.
In caso di mancata osservanza delle disposizioni di cui sopra e senza giustificate motivazioni, e fatte salve le inadempienze perseguite dal Codice Penale, l'incarico potrà essere revocato dandone motivato preavviso scritto all'interessato.

Art. 1.9 - MODALITÀ DI TRATTAMENTO DEI DATI

1. I dati in possesso del Comune di Bari possono essere trattati sia in modo informatizzato sia senza l'ausilio di strumenti elettronici o automatizzati. In ogni caso devono essere adottate tutte le misure necessarie a garanzia della sicurezza dei dati personali.

2. Al fine di tutelare la riservatezza delle persone, nelle ipotesi in cui la legge, lo Statuto o i regolamenti prevedano la pubblicazione obbligatoria di atti, documenti o provvedimenti, il Responsabile del trattamento, tenuto conto del *principio di necessità*, dovrà valutare se la finalità di trasparenza e di comunicazione può essere perseguita senza divulgare dati personali. Diversamente, dovrà rispettare l'ulteriore *principio di proporzionalità* per il quale i tipi di dati e il genere di operazioni svolte devono comunque essere *pertinenti e non eccedenti* rispetto alle finalità perseguite.

3. Il Titolare assicura adeguate garanzie in ordine al trattamento dei dati sensibili e/o giudiziari effettuato dal personale incaricato e/o da altri soggetti che operino per il Comune, in attuazione di quanto previsto dal *Codice Privacy*

4. E' vietata la diffusione di dati idonei a rivelare lo stato di salute[12] o il disagio economico-sociale dei soggetti *Interessati.*

5. E' parimenti vietata la diffusione e la comunicazione di dati personali a terzi in difetto di espressa disposizione di legge o regolamento. La comunicazione dei dati ad altri soggetti pubblici è ammessa anche in mancanza di una norma di legge o regolamento che lo preveda quando è comunque necessaria per lo svolgimento di funzioni istituzionali. In tal caso è necessario, ai sensi dell'art.39 del *Codice Privacy*, darne comunicazione al Garante.

6. Non si considera comunicazione la trasmissione e l'accesso ai dati da parte del personale incaricato delle varie articolazioni organizzative del Comune qualora il trasferimento e l'accesso avvenga per ragioni d'ufficio, nell'esercizio delle mansioni proprie di ciascun soggetto.

7. I Responsabili sono, tuttavia, tenuti ad adottare idonee e preventive misure al fine di limitare l'accesso e la trasmissione dei dati sensibili ai soli casi di effettiva necessità per lo svolgimento delle funzioni ed attività dell'Ente.

Art. 1.10 – CONTROLLI

1. A cura dei *Responsabili del trattamento* sono attivati controlli a carico dei propri *Incaricati*, con cadenza periodica ovvero quando ne ravveda l'opportunità, al fine di garantire la sicurezza delle *banche dati* e/o dei *dati personali* presenti nelle **Postazioni di Lavoro (PdL)** affidate a detti *Incaricati* oltre alla corretta gestione dei flussi operativi mediante i quali sono realizzati i trattamenti.

---

12 Vedi richiamato vigente "*Regolamento sul trattamento dei dati sensibili e/o giudiziari*" del Comune.

Art. 1.11 - AFFIDAMENTO A TERZI DI ATTIVITÀ O DI SERVIZI CHE IMPLICHINO IL TRATTAMENTO DI DATI PERSONALI

1. Al fine di tutelare i dati personali (ai sensi del Dlgs 196/03 e Disciplinare Tecnico Allegato B) di cui è Titolare il Comune di Bari, i Fornitori (soggetti terzi) di questa Amministrazione, che nell'espletamento dei servizi affidati possono accedere anche potenzialmente a banche dati, sono nominati Responsabili esterni del trattamento ex art. 29 del Dlgs 196/03.

2. È fatto obbligo, pertanto, ad ogni Responsabile- nella cui struttura di competenza ricade la necessità di affidare servizi che implicano il trattamento di dati personali a ditte esterne- di provvedere alla nomina delle stesse a Responsabile esterno del trattamento dei Dati, di custodire nomina, sottoscritta per accettazione, nel fascicolo "Protezione dei dati Personali" della propria struttura e di inviarne copia al Responsabile della Ripartizione Segreteria Generale Posizione Organizzativa Protezione dei Dati Personali.

3. Nel trattamento (anche potenziale) di eventuali "dati personali", il Soggetto terzo dovrà adempiere a tutte le misure previste dal DLgs. 196/2003, nonché a tutte le successive modifiche e/o integrazioni eventualmente introdotte nel periodo di vigenza contrattuale. Il Fornitore dovrà inoltre adeguarsi alle politiche di sicurezza adottate da questa Amministrazione, ancorché queste siano maggiormente impegnative rispetto alle misure minime previste dalla normativa vigente.

4. Il Titolare del trattamento dati si riserva il diritto di verificare l'applicazione delle misure sicurezza previste dalla normativa vigente presso i locali in cui si effettuano le attività di trattamento dei dati oggetto del contratto affidato, ancorché queste si svolgano al di fuori dei locali di questo Comune ed il Fornitore si impegna a mettere in atto tutte le misure necessarie all'espletamento di tali verifiche.

5. Alla cessazione del contratto, nel caso in cui i dati trattati in esecuzione del servizio affidato non siano già in possesso del Comune di Bari, il Fornitore consegnerà a questa Amministrazione tutti i dati in proprio possesso o l'integrazione a quelli già eventualmente nella disponibilità, relativi al contratto scaduto, sia che questi siano su supporto cartaceo che informatico. I dati dovranno essere consegnati in versione intelligibile e, nel caso si tratti di integrazioni, in modo tale che sia possibile una facile correlazione con quelli già in possesso.

6. Nel caso di dati consegnati su supporto informatico, questo dovrà essere leggibile con i comuni dispositivi informatici e con le specifiche del formato logico utilizzato per la memorizzazione dei dati. Quando i formati logici non siano di uso comune, ed in particolare quando siano utilizzati formati proprietari, il Fornitore dovrà rendere disponibili, senza alcun onere per questa Amministrazione, le procedure software applicative di lettura dei formati con i quali sono consegnati i dati, nonché gli eventuali software di base necessari.

7. Nel caso i dati siano ritenuti non più necessari all'espletamento della propria attività, il Titolare del trattamenti dati potrà rinunciare alla consegna dei dati da parte del Fornitore mediante comunicazione scritta. In seguito a verifica positiva della leggibilità dei dati trasmessi o alla rinuncia della consegna dei dati da parte del Fornitore, questa Amministrazione comunicherà per iscritto al Fornitore di procedere alla distruzione di tutti gli archivi in suo possesso, indicando il termine entro il quale effettuare tale operazione, se la conservazione di tali dati non sia prescritta al fornitore da specifica normativa vigente. Entro i termini previsti, il Fornitore comunicherà al Titolare del trattamento dati l'avvenuta distruzione dei dati in proprio possesso ovvero le motivazioni per le quali non abbia provveduto all'operazione.

Art. 1.12 – INFORMATIVA PUBBLICA

1. In caso di trattamento di dati personali, sensibili e giudiziari, i Responsabili del trattamento devono fornire all'interessato specifica informativa.
Nella modulistica d'ufficio, utilizzata dalle strutture comunali per l'acquisizione di dati personali, deve essere riportata idonea informativa ex art. 13 del Dlgs 196/03.

Art. 1.13 - DIRITTI DELL'INTERESSATO.

1. Alla "persona fisica" (art.40 del D.L. 6-12-2011 n.201), cui si riferiscono i dati personali sono garantiti i diritti previsti dall'art.7 del Codice Privacy, da esercitarsi con le modalità stabilite nei successivi artt. 8 e 9 del predetto Codice.

2. La richiesta di accesso ai dati personali che lo riguardano può essere inoltrata dall'Interessato al trattamento al Titolare o al Responsabile del trattamento senza formalità.

Art. 1.14 – SISTEMI DI VIDEOSORVEGLIANZA

1. L'attività di videosorveglianza deve essere esercitata nel rispetto delle disposizioni contenute nel D.Lgs. 30 Giugno 2003 n. 196, di seguito denominato "Codice della Privacy".

2. Le norme di seguito dispiegate garantiscono la conformità delle operazioni inerenti gli impianti visivi ai principi sanciti dal "Provvedimento in materia di videosorveglianza", emanato dall'Autorità Garante per la protezione dei dati personali, in data 8 aprile 2010, di seguito denominato "Provvedimento del Garante". In considerazione della necessità di salvaguardare i dipendenti di questo Comune da forme di controllo del loro operato, l'attività disciplinata dal presente testo viene svolta con attenzione al divieto di controllo a distanza dell'attività lavorativa. Qualora l'installazione degli impianti di cui all'art. 1 venga effettuata in aree nelle quali i dipendenti svolgano la loro prestazione lavorativa o che, comunque, siano abitualmente frequentate dagli stessi, è garantito il rispetto della disposizione dell'art. 4 co. 2 della L. 20 Maggio 1970, n. 300 (Statuto dei Lavoratori). Il Titolare del trattamento dei dati raccolti con i sistemi di videosorveglianza è il Comune di Bari. I Responsabili del trattamento sono le persone fisiche che esercitano funzioni direttive negli uffici in cui risultano installati i sistemi. Essi sono individuati dal Titolare ed a loro volta designano i soggetti Incaricati del trattamento i quali, a norma dell'art. 30 del Codice della Privacy, operano sotto la diretta autorità dei Responsabili.

3. Gli impianti di videoripresa ed i dati con essi raccolti devono essere salvaguardati, mediante adeguate misure di sicurezza, dai pericoli di distruzione, di perdita e di intrusione da parte di individui non autorizzati ad utilizzarli od a disporne il trattamento. Pur tuttavia la conservazione dei dati può avere un carattere esclusivamente temporaneo ed a tale principio non sono ammesse deroghe. I dati che possano soddisfare le finalità di tutela descritte nell'art. 3, dovranno essere conservati ed eventualmente utilizzati in un lasso di tempo strettamente necessario per conseguire gli scopi per cui sono raccolti, nel rispetto del principio di proporzionalità, ai sensi dell'art. 11 del Codice della Privacy. La conservazione non deve, comunque, superare l'arco temporale delle 24 (ventiquattro) ore dalla raccolta, fatta salva la necessità di ampliare il suddetto termine in occasione di chiusure degli uffici e festività o per soddisfare eventuali richieste dell'Autorità Giudiziaria, motivate dalla complessità delle indagini occorrenti ad individuare le modalità ed i responsabili della commissione di un fatto costituente reato.

4. I Responsabili del trattamento dati, in caso di installazione di impianti di videosorveglianza nelle sedi di competenza, devono rispettare una serie di obblighi imposti dalla Normativa a tutela della Privacy di seguito riportati :

- la raccolta e l'uso delle immagini sono consentiti solo se necessari allo svolgimento di

funzioni istituzionali e per il perseguimento di finalità di pertinenza dell'Azienda, tra i quali vi sono la sicurezza del patrimonio informativo e delle persone;

- i sistemi di videosorveglianza possono riprendere persone identificabili solo se, per raggiungere gli scopi prefissati, non possono essere utilizzati dati anonimi;
- tutti coloro che accedono ai locali video-sorvegliati devono essere opportunamente informati dell'esistenza di impianti di videosorveglianza nell'area in cui stanno per transitare. L'obbligo di informativa, come disposto dall'art. 13 del "Codice della Privacy", può essere adempiuto anche con una modalità semplificata, ossia con l'esposizione di cartelli indicanti la presenza nell'area di una o più telecamere. I cartelli devono essere collocati in posizione antistante i sistemi di videosorveglianza e devono avere dimensione caratteri alfabetici tali da essere chiaramente visibili anche in condizioni di scarsa od insufficiente illuminazione; essi devono anche recare l'indicazione se l'attività è limitata alla sola ripresa o si estende anche alla registrazione delle immagini. L'informativa deve indicare le finalità dell'installazione degli impianti visivi, citate nel precedente art. 2, le modalità di "trattamento dei dati" con essi raccolti, nonché i soggetti che rivestono i ruoli di Titolare e Responsabili del trattamento.
- Il Responsabile del trattamento deve nominare Responsabile della videosorveglianza l'incaricato all'accesso al sistema di videosorveglianza
- Il Responsabile del trattamento predispone il DAV - documento sull'attività di videosorveglianza e custodisce l'attestazione di conformità dell'impianto rilasciato dall'installatore.
- Il Responsabile del trattamento nomina, se presente, la ditta manutentrice dell'impianto di videosorveglianza in qualità di Amministratore di Sistema.
- Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa. Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero èrichiesta per la sicurezza del lavoro (art. 4 Legge n. 300/1970; art. 2 D.Lgs n. 165/2001); è inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad es. bagni, spogliatoi, docce, armadietti etc..). Non è ammessa la presenza di telecamere finte per soli fini di deterrenza.

Art. 1.15 – MISURE DI SICUREZZA

1. I Responsabili del Trattamento anche con l'ausilio del personale della Ripartizione Innovazione Tecnologica, adottano, nell'ambito delle articolazioni organizzative cui sono preposti in relazione allo sviluppo tecnologico ed all'evoluzione del quadro normativo di riferimento, idonee disposizioni organizzative e preventive misure di sicurezza per il trattamento dei dati, conformandosi al "Codice Privacy" ed al seguente "Disciplinare d'uso" al fine di:

a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati, ivi compresi quelli memorizzati su supporti magnetici e ottici, nonché delle banche dati e dei locali ove le stesse sono collocate;
b) evitare l'accesso non autorizzato agli archivi, alle banche dati, alla rete e, in generale, ai servizi informatici del Comune vietando, in particolare, in mancanza di preventiva autorizzazione e di idonei accorgimenti, l'installazione di dispositivi di connessione a reti esterne su personal computer collegati alla LAN-WAN (rete locale-geografica comunale);
c) prevenire trattamenti di dati non conformi alla legge o ai regolamenti.

2. In particolare, nell'individuazione delle "misure minime di sicurezza", ciascun Responsabile del trattamento tiene conto:

- della peculiarità dei dati raccolti, detenuti o trattati;
- della tipologia, cartacea o informatizzata, delle banche dati;
- dello sviluppo tecnologico della strumentazione in dotazione alla propria struttura;
- dell'abilità e professionalità degli operatori incaricati.

3. In caso di trattamento di dati personali mediante sistemi di videosorveglianza, il Responsabile del trattamento, in conformità alle previsioni della vigente normativa in materia di videosorveglianza, adotta idonee e preventive misure di sicurezza volte a ridurre al minimo i rischi di distruzione, perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 1.16 – ACCESSO A DOCUMENTI AMMINISTRATIVI.

1. In materia di diritto di accesso ai documenti amministrativi (ai sensi dell'art.2 della Legge 241/1990 integrata con Legge 15/2005), il principio di trasparenza può prevalere sulla tutela della riservatezza, consentendo al legittimo titolare del diritto di accedere anche ai documenti contenenti dati personali di terzi la cui conoscenza sia necessaria per la cura o la difesa dei suoi interessi giuridici.

2. Nel caso di istanza di accesso a documenti contenenti dati idonei a rivelare lo stato di salute e la vita sessuale di terzi, l'accesso è consentito solamente se la situazione giuridicamente rilevante che si intende tutelare è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 1.17 – FUNZIONI DI COORDINAMENTO E SUPPORTO

1. Al fine di garantire il costante aggiornamento ed adeguamento dell'attività del Comune di Bari alla vigente normativa in materia di protezione dei dati personali, viene demandato al Dirigente della Ripartizione Segreteria Generale Posizione Organizzativa Protezione dei Dati Personali, il coordinamento di tutte le disposizioni organizzative in materia di Privacy ed il supporto a tutto il personale per i necessari approfondimenti di carattere interpretativo ed operativo.

2. – DISCIPLINARE INTERNO

PREMESSA

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, **il Comune di Bari con il presente atto adotta un DISCIPLINARE INTERNO diretto ad evitare che comportamenti inconsapevoli possano innescare problemi alla gestione della R*ete informatica comunale* e/o minacce alla *sicurezza nel trattamento dei Dati Personali* di qualsivoglia tipo *(personale, sensibile e giudiziario*).**

La progressiva diffusione delle nuove tecnologie informatiche ed, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone *la Rete del Comune di Bari* a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul *diritto d'autore* e legge sulla *privacy*, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Ente stesso.

Pertanto le prescrizioni di seguito previste, in presenza o meno della dotazione informatica, si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D.Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni indicate nel precedente Regolamento in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze che possono scaturire sul piano personale in caso di violazione delle stesse.

CAMPO DI APPLICAZIONE

Il presente DISCIPLINARE D'USO DELLA "DOCUMENTAZIONE CARTACEA" E DELLA "DOTAZIONE INFORMATICA" si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con lo stesso intrattenuto (consulente, collaboratori a progetto, in stage, ecc.).
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (borsista, stagista, consulente ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche essere indicata quale ***"Incaricato del trattamento"*** ai sensi dell'art. 30 del Dlgs 196/03.

2.a) USO DELLA DOCUMENTAZIONE CARTACEA

Art. 2a.1 – MODALITÀ OPERATIVA.

I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. in armadi o in cassetti chiusi a chiave).
I dati, le cartelle ed appunti vari, contenti dati personali, devono sostare sulle scrivanie solo il tempo necessario al loro trattamento. I documenti contenenti dati personali, che vengono prelevati dagli archivi per l'attività quotidiana, devono esservi riposti a fine giornata. I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

Art. 2a.2 – MISURE DI SICUREZZA.

Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

Art. 2a.3 – DISTRUZIONE.

Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

2.b) USO DELLA DOTAZIONE INFORMATICA

Art. 2b.1 - Utilizzo del Personal Computer.

1. Il Personal Computer affidato all'Utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il Personal Computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

2. Il Personal Computer dato in affidamento all'Utente permette l'accesso alla rete del Comune di Bari solo attraverso specifiche credenziali di accesso ed autenticazione come meglio descritto al successivo Art. 2b.2 del presente Mansionario.

3. Il Comune di Bari rende noto che il personale della Ripartizione Innovazione Tecnologica ovvero gli incaricati esterni da questi delegati è autorizzato a compiere interventi nel sistema informatico, diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad esempio: aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi artt. 2b.6, comma 4 e 2b.7, comma 1, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata od impedimento del dipendente.

4. Il personale della Ripartizione Innovazione Tecnologica, ovvero gli incaricati esterni da questi delegati, ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, e malware in genere. L'intervento viene effettuato esclusivamente su chiamata dell'Utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data formale comunicazione della necessità dell'intervento stesso.

5. Salvo preventiva espressa formale autorizzazione del Responsabile della Ripartizione Innovazione Tecnologica non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale tecnico per conto dell'Ente, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone il Comune di Bari a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

6. Parimenti al comma precedente, non è consentito all'Utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, Internet key ...) oltre a quelli componenti la configurazione fisica dell'Hw della PdL ricevuta in uso.

7. Ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale tecnico preposto nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo Art. 2b.8 del presente Mansionario relativo alle procedure di protezione antivirus.

8. Non è consentito collegare alla rete del Comune di Bari Personal Computer o Pc Portatili e, più in generale, qualsiasi dispositivo hardware senza la formale autorizzazione del richiamato Responsabile. Eventuali acquisiti di personal computer devono essere necessariamente comunicati alla Ripartizione Innovazione Tecnologica che provvederà a predisporre l'installazione e la configurazione degli stessi in totale sicurezza.

Art. 2b.2 - assegnazione e Gestione delle credenziali di accesso al PC e di autenticazione nella intranet

1. Le credenziali di autenticazione nella intranet (accesso rete comunale), vengono inizialmente assegnate dal personale della Ripartizione Innovazione Tecnologica e successivamente obbligatoriamente reimpostate dal dipendente stesso secondo criteri prestabiliti dalla normativa vigente e con modalità operative di cui ai commi successivi. Non sono ammesse impostazioni autonome della password al Bios del Pc onde evitare impedimenti all'accesso al Pc in caso di prolungata assenza dell'incaricato e considerata la necessità di questa Amministrazione, di garantire in ogni caso la continuità dei servizi istituzionali.

2. La credenziale di autenticazione (login) consiste in un codice per l'identificazione dell'Utente (user id), assegnato dal personale tecnico ed associato ad una parola chiave (password) riservata e modificata dall'Incaricato, Utente di Rete. Essa dovrà essere memorizzata, custodita con la massima diligenza e non divulgata.

3. La parola chiave deve essere formata da 8 o più caratteri appartenenti ad almeno tre delle seguenti quattro categorie: lettere maiuscole, lettere minuscole, numeri, caratteri speciali, anche in combinazione fra loro e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4. La password di accesso di ciascun Utente di rete sarà automaticamente reimpostata ogni tre mesi. In base a tale procedura automatica, l'Utente, mediante avviso a video, dovrà inserire entro e non oltre la scadenza mostrata a video, una nuova password, diversa dalla precedente, pena il blocco del PC con conseguentemente inibizione dell'accesso alla intranet comunale.

5. L'Utente potrà richiedere la modifica della parola chiave al personale tecnico autorizzato, per decorrenza del termine sopra previsto in via eccezionale e/o in via ordinaria in caso questi ravveda una perdita della riservatezza.

6. L'utente non è amministratore locale del PC

Art. 2b.3 - Utilizzo della Rete

1. Per l'accesso alla Rete (intranet comunale) ciascun Utente deve essere in possesso delle specifiche credenziali sopra descritte.

2. È assolutamente proibito accedere alla rete informatica comunale e/o nei programmi con un codice d'identificazione Utente di un altro operatore.

3. La presenza di eventuali cartelle di rete condivise sono da considerarsi strumento di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.

4. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco o più dischi fissi C:, D: ecc. del proprio PC e fintanto non si provveda diversamente) non sono soggette a salvataggio da parte del personale della Ripartizione Innovazione Tecnologica. Pertanto la responsabilità del salvataggio dei dati, almeno settimanalmente, è a carico del singolo Utente. Eventuali eccezioni sono da concordare con l'Amministratore di Sistema.

5. Il personale tecnico autorizzato può in qualunque momento, senza preavviso, procedere alla rimozione dai PC in rete di ogni file e/o applicazione che riterrà essere pericolosi per la sicurezza dei dati e della rete.

Art. 2b.4 - Utilizzo e conservazione dei supporti rimovibili

1. Eventuali supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi a chiave.

2. E' vietato l'utilizzo di supporti rimovibili personali (dischi rigidi e penne USB) compreso qualsiasi altro punto di memorizzazione tramite internet (detto "storage on line") nel caso si voglia trattare dati personali, sensibili e/o giudiziari. In caso di trasferimento dei citati dati fra pdl in rete, si devono utilizzare "cartelle di lavoro condivise" e protette da password note solo agli utenti a ciò interessati.

3. L'Utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Art. 2b.5 - Utilizzo di PC portatili

1. L'Utente è responsabile del PC portatile eventualmente assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nei luoghi di lavoro.

2. Ai PC portatili autorizzati si applicano le regole di utilizzo previste dal presente Disciplinare, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

3. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

4. Tali disposizioni si applicano anche nei confronti di incaricati esterni.

5. E' vietato connettersi alla rete attraverso qualsiasi dispositivo personale (PC portatile, smartphone, tablet etc.) non preventivamente autorizzato dal Responsabile della Ripartizione Innovazione Tecnologica .

Art. 2b.6 - Uso della posta elettronica

1. La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2. È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare la posta elettronica ordinaria e certificata per:
-l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
-l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti,sondaggi e aste on-line;
-la partecipazione a catene di sant'Antonio; non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

3. La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti (in termini di centinaia di MB e, ancor più di GB).

4. È obbligatorio porre la massima attenzione nell'aprire i file allegati alle e-mail (detti attachments) prima del loro utilizzo. In linea di massima (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti, altrimenti, se obbligati sottoporre necessariamente detti file ad una "scansione approfondita" dell'antivirus prima del loro utilizzo.

5. Nel caso in cui un Utente, dotato di email si assenti per più giorni (ad es. per malattia), sarà consentito al suo competente Responsabile accedere alla casella di posta elettronica, al fine di garantire la continuità lavorativa e comunque nel rispetto del principio di necessità e di proporzionalità. Le attività di accesso dovranno essere verbalizzate dal Responsabile del Servizio e l'incaricato, al rientro, dovrà essere opportunamente informato.

Art. 2b.7 - Navigazione in Internet

1. Il PC assegnato al dipendente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile **esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa all'interno dell'Ente.

2. In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare Internet per:
- l'upload o il download di software gratuiti se non espressamente autorizzati dal competente Responsabile della Ripartizione Innovazione Tecnologica ;
-l 'utilizzo di documenti (filmati e musica) provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi autorizzati e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a forum non professionali, a giochi on-line, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Comune di Bari adotta uno specifico sistema di filtro automatico che impedisce determinate operazioni quali l'upload, download (illeciti o illegali) o l'accesso a determinati siti (black-list).

4. Gli eventuali controlli per motivi di sicurezza informatica, compiuti dall'Amministratore di Sistema, potranno avvenire mediante un sistema di controllo dinamico dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui log, i quali sono cancellati periodicamente ed automaticamente, non è sistematico e le informazioni vengono conservate temporaneamente per finalità di sicurezza di questa Amministrazione. Il prolungamento dei tempi di conservazione dei log potrà aver luogo solo nei seguenti casi :
-esigenze tecniche o di sicurezza del tutto particolari ;

-indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
-su specifica richiesta dell'autorità giudiziaria

Art. 2b.8 - Protezione antivirus

1. Il sistema informatico del Comune di Bari è protetto da software antivirus aggiornato quotidianamente. Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico. Questa fattispecie può accadere mediante virus o malware, proveniente da dati e/o software importati/installati dall'Utente, che si auto installano, all'insaputa dell'Utente, all'interno del Pc, infettandolo e diffondendosi nella nella rete informatica comunale.

2. Nel caso in cui il software antivirus rilevi e non disinfetti la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare l'accaduto al personale autorizzato della Ripartizione Innovazione Tecnologica.

3. Ogni dispositivo di memorizzazione esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale tecnico autorizzato che provvederà ad effettuare le dovute operazioni di disinfezione.

Art. 2b.9 - Osservanza delle disposizioni in materia di Privacy

1. E'obbligatorio attenersi alle disposizioni in materia di Privacy ed alle misure minime di sicurezza, come indicato nella "lettera di designazione" ad Incaricato del trattamento dei dati ai sensi del citato Disciplinare Tecnico allegato B) al D.Lgs. n. 196/2003.

Art. 2b.10 - Accesso agli strumenti e dati informatici trattati dall'utente

1. Oltre che per motivi di sicurezza del Sistema Informatico del Comune, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo prima descritte, comunque estranea a qualsiasi monitoraggio dell'attività lavorativa, è facoltà del personale della Ripartizione Innovazione Tecnologica, ivi compreso il personale di società esterne, sempre nel rispetto della normativa sulla Privacy e della Legge 300/70, accedere direttamente a tutti gli strumenti informatici ed al loro contenuto.

Art. 2b.11 - Sistemi di controlli graduali

1. In caso di anomalie, il personale incaricato tecnico autorizzato della Ripartizione Innovazione Tecnologica effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti del settore in cui è stata rilevata l'anomalia, si evidenzierà l'utilizzo irregolare degli strumenti informatici e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

2. In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Art. 2b.12 – Sanzioni

È fatto obbligo a tutti i dipendenti ed utenti del sistema informativo del COMUNE DI BARI di osservare le disposizioni portate a conoscenza con il presente Disciplinare. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

3.- Aggiornamento , revisione , pubblicità ed Entrata in vigore

Art. 3.1 – Aggiornamento , revisione , pubblicità ed entrata in vigore del presente documento "Disposizioni in materia di protezione dei dati personali e Disciplinare interno sull'utilizzo della documentazione cartacea e della dotazione informatica"

1. Il presente Documento "Disposizioni in materia di protezione dei dati personali e Disciplinare interno sull'utilizzo della documentazione cartacea e della dotazione informatica", di seguito "Disposizioni", è stato redatto tenendo conto del D.Lgs 196/2003, delle linee guida del Garante della Privacy emanate con delibera n. 13 del 1° marzo 2007 e della direttiva n.2/2009 del Ministro per la Pubblica Amministrazione e Innovazione.

2. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente documento. Le proposte saranno esaminate dai Responsabili delle Ripartizioni di competenza.

3. Le presenti Disposizioni con annesso Disciplinare sono soggetti a revisione come per Legge o qualora se ne ravveda la necessità.

4. Copia del presente documento verrà consegnata a ciascun dipendente comunale della rete informatica comunale, ovvero messo a disposizione per ogni Utente generico autorizzato, a cura del Responsabile della Ripartizione Segreteria Generale-POS Protezione dei Dati Personali ad avvenuta approvazione dello stesso da parte della Giunta Comunale.

5. Con l'entrata in vigore del presente Documento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.