C I T T A ’ DI M A N F R E D O N I A

(Provincia di Foggia)

DOCUMENTO PROGRAMMATICO DI SICUREZZA

PARERI DEI RESPONSABILI DEL TRATTAMENTO DEI DATI:

(D.L.vo 196/2003)

Direttore Generale	(Avv. Dario Melillo)	Favorevole _____
Segretario Generale	(Dott. Pietro Lo mastro)	Favorevole _____
Dirigente 1° Settore	(Dott. Matteo Ognissanti)	Favorevole _____
Dirigente 2° Settore	(Dott. Matteo Di Benedetto)	Favorevole _____
Dirigente 3° Settore	(Dott. Francesco Zoccano)	Favorevole _____
Dirigente 4° Settore	(Dott. Mariano Ciritella)	Favorevole _____
Dirigente 5° Settore	(D.ssa Maria Siponta Ciuffreda)	Favorevole _____
Dirigente 6° Settore	(Ing. Simone Lorussi)	Favorevole _____
Dirigente 7° Settore	(Ing. Domenico Curci)	Favorevole _____
Dirigente 8° Settore	(Ing. Giovanni Spagnuolo)	Favorevole _____

INDICE

Premessa

Con il termine "sicurezza" si intende l'insieme di misure, di carattere organizzativo e tecnologico, tese ad assicurare a ciascun utente autorizzato (e a nessun altro) esclusivamente i servizi previsti per l'utente stesso, nei tempi e nelle modalità stabilite.

Più formalmente, secondo la nota definizione ISO, la sicurezza è l'insieme delle misure atte a garantire l'insieme di tutte le misure atte a difendere il Sistema Informativo dalle possibili minacce d'attacco, con particolare riferimento a:

- *Disponibilità:* l'informazione ed i servizi che eroga devono essere a disposizione degli utenti del sistema compatibilmente con le autorizzazioni.

- *Integrità:* l'informazione ed i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione.

- *Riservatezza:* l'informazione che contiene può essere fruita solo dalle persone autorizzate a compiere tale operazione.

Gli incidenti di sicurezza possono essere identificati come *accidentali* o *deliberati* e possono essere causati da:

- malfunzionamenti di sistemi hardware e software, applicativi software e servizi;

- persone esterne all'organizzazione (hacker, spie, terroristi, vandali, ecc);

- eventi naturali (inondazioni, incendi, terremoti, tempeste, ecc);

- persone interne all'organizzazione.

L'approccio globale alla sicurezza richiede di considerare gli aspetti tecnici (sicurezza fisica e logica), strategici (obiettivi e budget), organizzativi (definizione di ruoli, procedure, formazione), economici (analisi dei costi) ed infine legali (leggi e decreti, provvedimenti Garante Privacy).

In particolare è necessario che:

1. Tutti le componenti informatiche, hardware e software, debbano garantire che ogni loro mal funzionamento o messa fuori operazione non comporti una diminuzione della sicurezza di esercizio;

2. Le responsabilità dell'esercizio e dei controlli interni di sicurezza siano affidate a persone distinte e collocate nella struttura organizzativa comunale;

3. Sia sempre possibile individuare, inequivocabilmente l'autore di una qualsiasi operazione;

4. Sia sempre possibile ripristinare il sistema di fronte a guasti o eventi, naturali o dolosi, allo stato in cui si trovava, prima del verificarsi dell'evento stesso, di un certo tempo concordato a priori tra le parti;

Rendere sicuro un Sistema Informativo non significa esclusivamente attivare un insieme di contromisure specifiche, di carattere tecnologico ed organizzativo, che neutralizzino tutti gli attacchi ipotizzabili al sistema di servizi, ma significa, in particolare, collocare ciascuna delle contromisure individuate in una politica organica di sicurezza che tenga conto dei vincoli (tecnici, logistici, organizzativi, amministrativi e legislativi) imposti dalla struttura tecnica ed organizzativa in cui il sistema di servizi opera e che giustifichi ciascuna contromisura in un quadro complessivo.

Nel presente Documento Programmatico sulla Sicurezza, da redigere entro il 31 marzo di ogni anno, sono contenute idonee informazioni atte a garantire l'osservazione delle misure minime di sicurezza descrivendo:

1. L'elenco dei trattamenti di dati personali;

2. La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

3. L'analisi dei rischi che incombono sui dati;

4. Le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

5. La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;

6. La previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

7. La descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

Art. 1
(Sistema Informativo Automatizzato sicuro)

Ai fini dell'articolo 4 del *Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali* si intende per:

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "interessato", la persona fisica, la persona giuridica, lente o l'associazione cui si riferiscono i dati personali;

j) “comunicazione”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

k) “diffusione”, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

l) “dato anonimo”, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

m) “blocco”, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

n) “banca di dati”, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

o) “Garante”, l’autorità di cui all’articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Art. 2
(Titolare)

1. Il Comune di Manfredonia è il Titolare dei dati personali gestiti dalle proprie articolazioni organizzative e delle relative banche dati ed è rappresentato, ai fini previsti dalla legge, dal Sindaco.

2. Ai sensi del Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche ed integrazioni e del presente regolamento il titolare provvede a:

   - comunicare al Garante per la protezione dei dati personali le attività individuate per le quali non è determinata dalla legge una corrispondente rilevante finalità di interesse pubblico;

   - formulare, per iscritto, le istruzioni e le direttive di massima rivolte ai responsabili ed agli incaricati;

   - controllare la corretta applicazione della legge, delle istruzioni e delle direttive impartite;

   - essere a conoscenza delle banche dati, personali e sensibili, esistenti ed i nominativi dei rispettivi responsabili ed incaricati.

3. Il Titolare è comunque responsabile di:

   - Decisioni sulle finalità di raccolta dati.

   - Decisioni sulle modalità del trattamento dei dati.

   - Emanazione di norme di sicurezza e salvaguardia dell'integrità dei dati.

   - Adempimenti e obblighi che la legge gli attribuisce espressamente in via esclusiva o in concorso con i responsabili designati.

   - Mancata vigilanza sulla esecuzione degli adempimenti legittimamente assegnati ai Responsabili.

   - Verifica del rispetto da parte dei responsabili degli obblighi di legge e delle istruzioni scritte ricevute.

Art. 3
(Responsabili)

1. Il Direttore Generale, il Segretario Generale e i Dirigenti dei Settori sono responsabili di tutte le banche dati esistenti nei settori e negli uffici di loro competenza, nonché dei relativi trattamenti. Il titolare può designare altri responsabili, ai sensi dell'art. 5 comma 2 del Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche ed integrazioni.

2. I Responsabili per il trattamento dei dati che, ai fini della responsabilità attribuita sono tutti domiciliati presso la sede del Comune di Manfredonia, provvedono, per i rispettivi ambiti di competenza, a tutte le attività previste dalla legge ed in particolare a:

   - individuare e, se ritenuto opportuno, comunicare al Sindaco i nominativi dei soggetti incaricati del trattamento dei dati, anche non nominativamente e con riferimento a categorie o specifici profili di operatori e alla loro collocazione organizzativa;

   - fornire agli incaricati, per iscritto, sulla base delle direttive di massima impartite dal titolare, le istruzioni per il corretto trattamento dei dati personali, eseguendo gli opportuni controlli;

   - adottare le misure e disporre gli interventi necessari per la sicurezza della conservazione dei dati e per la correttezza dell'accesso sulla base delle direttive a tale scopo impartite dal responsabile del Servizio Sistemi Informativi dell'Ente;

   - adottare le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato;

- inviare al Garante, tramite il Titolare, le comunicazione e le notificazioni previste dalla parte I, Titolo VI del Decreto Legislativo n. 196/2003;

- stabilire le modalità di gestione e le forme di responsabilità relative a banche dati condivise da più articolazioni organizzative, d'intesa con gli altri responsabili. In caso di mancato accordo, sentiti i responsabili, decide il Direttore Generale;

- individuare le tipologie di dati sensibili assoggettabili a trattamento secondo e le operazioni su di essi eseguibili;

- per il corretto trattamento dei dati contenuti su Personal Computer; il Responsabile deve garantire che le postazioni informatiche siano conformi a quanto indicato nel *Disciplinare tecnico in materia di misure minime di sicurezza* (allegato B del Codice). A tal fine le caratteristiche di nuovi personal computer da collegare alla rete comunale dovranno essere concordate con il servizio Sistemi Informativi e Statistica.

3. Il Responsabile ha il dovere di compiere quanto necessario ai fini del rispetto e della corretta applicazione del DLGS 196/2003 e può esercitare, in tal senso, autonomi poteri gestionali e di controllo.

4. E' compito del Responsabile vigilare affinché venga impedito l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o in cui avvengono trattamenti di dati.

5. E' altresì suo compito impedire che vengano introdotti in tali aree oggetti, apparecchiature, sostanze o materiali che possono favorire la realizzazione dei rischi sopra individuati, ovvero non indispensabili allo svolgimento dell'attività lavorativa.

6. L'accesso e la permanenza di personale addetto ad attività di servizio (pulizia, manutenzioni, etc.) deve avvenire con procedure e controlli idonei a ridurre i rischi sopra individuati.

Art. 5
(Responsabile della sicurezza informatica)

1. Il Responsabile della sicurezza informatica, nominato da Titolare provvede ad assicurare le misure di sicurezza degli archivi informatici al fine di:

   - ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati su supponi magnetici o ottici gestiti, nonché delle banche dati e dei locali ove sono collocate;

- evitare l'accesso non autorizzato alle banche dati, alla rete e, in generale, ai servizi informatici del Comune;

- prevenire trattamenti dei dati non conformi alla legge o ai regolamenti e la cessione o distribuzione dei dati in caso di cessazione del trattamento.

2. A tal fine con il Responsabile della sicurezza informatica si avvale della collaborazione dei dipendenti del servizio Sistemi Informativi e di almeno un referente per ogni Settore che, in base alle proprie conoscenze tecniche e alle istruzioni ricevute assicurano il rispetto delle misure di sicurezza del Settore di appartenenza.

Art. 6
(Incaricati)

1. I Responsabili per il trattamento dei dati procedono all'individuazione all'interno dei singoli Settori degli Incaricati, persone autorizzate nei vari uffici a compiere le operazioni di trattamento dei dati, da svolgersi secondo le modalità previste dalla legge.

2. Gli Incaricati mettono in atto le istruzioni e i compiti definiti dalla legge e dal Responsabile del Trattamento di competenza; relativamente al trattamento dei dati elettronici, devono dar conto anche al Responsabile della sicurezza informatica del rispetto delle disposizioni emanate.

3. Tutti i dipendenti del Comune di Manfredonia sono incaricati del trattamento dei dati sulla base delle competenze assegnate nell'ambito dell'organizzazione comunale, delle esigenze di servizio esplicitate in appositi ordini, conformemente alla necessità di trattamento e con il minimo livello di conoscenza necessario dei dati.

4. Il trattamento dei dati è vincolato al rispetto del segreto d'ufficio nonché ai doveri di correttezza nell'adempimento delle prestazioni come previste dal contratto e dal codice di comportamento dei dipendenti delle pubbliche amministrazioni.

5. E' compito degli Incaricati:

   a) impedire l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro di propria competenza, con particolare attenzione agli spazi in cui vengono custodite banche dati o in cui avvengono trattamenti di dati.

   b) trattare i dati diligentemente, evitando accessi indebiti da parte di estranei non autorizzati o non incaricati del trattamento. Al termine dell'utilizzo i documenti contenenti i dati vanno ricollocati nei rispettivi contenitori e/o archivi affinché gli atti e documenti contenenti dati sensibili utilizzati dagli incaricati (solo ed

esclusivamente per compiti d'ufficio) siano conservati in contenitori muniti di serratura;

c) predisporre quanto necessario affinché i contenitori (armadi, schedari e simili) contenenti dati personali vengano sempre chiusi a chiave dopo l'utilizzo; così pure che ciò avvenga per i locali in cui vengono archiviati dati personali; inoltre devono conservare le chiavi degli armadi, schedari, cassettiere ed archivi anche presso il Responsabile del trattamento competente oppure in luogo all'interno del Settore conosciuto solamente dagli incaricati interessati e dai rispettivi Responsabili del trattamento;

d) predisporre quanto necessario, seguendo le indicazioni dell'Amministratore del sistema, per il corretto trattamento di dati personali contenuti in banche dati ubicate su elaboratori (PC) non accessibili da altri elaboratori (assumendo in tale veste il ruolo di Amministratore del sistema);

e) predisporre in caso di necessità una relazione scritta in ordine a tutti gli adempimenti eseguiti ai sensi del DLGS 196/2003, alla documentazione raccolta ed archiviata ai sensi della medesima legge, nonché in ordine alle misure di sicurezza. Tale relazione dovrà essere, successivamente, trasmessa al Titolare del trattamento;

f) distruggere i dati personali in caso di cessazione del trattamento degli stessi, provvedendo alle necessarie formalità;

g) segnalare la correttezza dei dispositivi antincendio per i locali e/o i siti in cui hanno sede le banche dati contenenti i dati personali e dare pronta comunicazione al Titolare in caso di interventi di adeguamento;

6. Ogni incaricato deve garantire la disponibilità dei dati che tratta in caso di propria assenza o impedimento, al fine di garantire il principio di fruibilità da parte di chi ha diritto di conoscerli ed utilizzarli.

7. Non è considerata comunicazione né violazione della normativa vigente la conoscenza dei dati personali da parte degli Incaricati a compiere le operazioni del trattamento, che operano per designazione scritta dal Titolare o dal Responsabile.

8. Nei casi di particolari trattamenti (attività giornalistica, trattamento per scopi storici, statistica), gli incaricati dovranno attenersi anche a quanto stabilito nei rispettivi codici di Deontologia allegati A1, A2 e A3 del *Codice in materia di protezione dei dati personali.*

Art. 7
(Norme di gestione dei personal computer del Comune di Manfredonia)

1. Il Servizio Sistemi Informativi e Statistica Comunale provvede ad assicurare lo sviluppo delle misure di sicurezza degli archivi informatici.

2. A tal fine dovranno essere rigorosamente rispettate le seguenti regole da tutti coloro a cui sono assegnate postazioni di lavoro informatiche presso le strutture del Comune di Manfredonia:

   a) Le caratteristiche tecniche delle postazioni informatiche devono essere concordate con il Servizio Sistemi Informativi prima della procedura di acquisizione.

   b) Ad ogni personal computer collegato al Sistema Informativo comunale viene assegnato un indirizzo di rete univoco che consente l'accesso alla rete comunale da non modificare. In caso contrario la persona a cui è assegnato il Personal Computer risponde personalmente di eventuali conseguenze sulla vulnerabilità della rete.

   c) Ad ogni persona avente titolo, il servizio Sistemi Informativi assegna un *account* personale (utente e password) per consentire l'accesso alle risorse della rete del Comune. Tale *account* è rigorosamente personale. Ogni utente dovrà garantire la riservatezza della propria password ed impedire che altri possano utilizzarla.

   d) Su ogni postazione di rete deve essere installato un programma Antivirus, secondo disposizioni del servizio Sistemi Informativi. E' cura dell'operatore verificare che tale sistema sia sempre presente e aggiornato.

   e) E' assolutamente vietato installare sul proprio computer programmi ricevuti dall'esterno. In caso contrario la persona a cui è assegnato il Personal Computer risponde personalmente di eventuali conseguenze sulla vulnerabilità della rete.

   f) Il salvataggio periodico dei dati trattati su Personal Computer dovrà essere eseguito dalla persona a cui è assegnato il Personal Computer. In caso di archivi condivisi in rete, il salvataggio dei dati deve essere eseguito e custodito da apposito personale indicato dal Responsabile del trattamento dati. Le specifiche del salvataggio delle banche dati informatiche possono essere concordate con il Servizio Sistemi Informativi e Statistica.

   g) Non e possibile connettere apparecchi aggiuntivi alla rete, senza che sia stato richiesto ed assegnato da parte degli addetti del Servizio Sistemi Informativi il relativo indirizzo di rete costituito dal numero IP e dal nome associato. Ciò vale non solo per i Personal Computer (compresi i portatili), ma per ogni altro apparecchio (stampanti di rete, terminal server, router, etc.). Qualunque intervento sul cablaggio di rete, deve essere concordato con gli addetti del Servizio Sistemi Informativi, autorizzato e verificato dopo la realizzazione.

h) E' assolutamente vietato utilizzare, per il collegamento alla rete Internet, modem o router collegati direttamente al proprio Personal Computer. In caso contrario la persona a cui è assegnato il Personal Computer risponde personalmente di eventuali conseguenze sulla vulnerabilità della rete.

i) In caso di inosservanza delle nonne di utilizzo della rete, il servizio Sistemi Informativi non garantirà la sicurezza di tutta la rete informatica del Comune di Manfredonia.

j) In caso di reiterata inosservanza, per colpa grave o dolo, il trasgressore sarà suscettibile di provvedimento disciplinare secondo la normativa vigente.

k) In caso di misure d'emergenza, tese a salvaguardare il funzionamento della rete nel suo insieme o in una delle sue parti il servizio Sistemi Informativi e Statistica può, come misura transitoria, attuare una sospensione parziale o totale all'accesso alla rete di una singola postazione o di parte della rete.

Art. 8
(Norme di utilizzo dei personal computer del Comune di Manfredonia)

1. Per accedere al proprio computer è necessario creare e usare una password sicura, composta da almeno 8 caratteri, con lettere maiuscole e minuscole, numeri e simboli da cambiare ogni sei mesi.

2. Utilizzare uno screensaver, protetto tramite password. In questo modo si eviterà che altre persone accedano alle informazioni quando si è momentaneamente assenti. Impostare la funzione di attivazione automatica a non più di 10 minuti.

3. Spegnere sempre il Personal Computer al termine della giornata di lavoro o al termine dell'utilizzo.

4. Utilizzare sempre un software Antivirus aggiornato e autorizzato, soprattutto su computer collegati a Internet.

5. Controllare sempre i files provenienti dall'esterno tramite software Antivirus.

6. Prestare molta attenzione quando si ricevono messaggi di posta elettronica con allegati da mittenti sconosciuti. Gli allegati possono contenere virus o altri programmi dannosi.

7. Non accedere a dati, server o account per i quali non si è autorizzati.

8. Non inviare messaggi di posta non sollecitati o materiale vario a destinatari che non abbiano richiesto tale materiale.

9. L'accesso alla rete Internet e le relative modalità dovranno essere autorizzate dal Responsabile. In tal caso, per evitare l'attacco da parte di virus o altre situazioni che provocherebbero problemi anche alle altre postazioni della rete comunale si raccomanda consultare soltanto siti istituzionali, evitando:

   a) Siti con contenuti vietati

   b) Siti web che offrono sfondi per il desktop del PC

   c) Siti che offrono loghi e/o suonerie per cellulari

   d) Siti web che offrono brani MP3 e clip video

   e) Di scaricare messaggi di posta elettronica (mail) provenienti da mittenti sconosciuti, con oggetto in lingua straniera con allegati ".exe" o comunque sospetti

   f) Di scaricare file di dimensioni molto grandi che occupano per molto tempo la linea di collegamento, rallentando la trasmissione agli altri utenti.

Art. 9
(Trattamento dei dati in formato elettronico)

I sistemi di accesso agli archivi strutturati sono costituiti da programmi specifici, detti anche *procedure*, che permettono di inserire, modificare, interrogare, leggere e stampare le informazioni in essi contenute.

La proprietà dei dati è del Titolare, la gestione è del Responsabile, l'amministrazione dei dati è dell'Incaricato, sotto il coordinamento del Servizio Sistemi Informativi che detiene il sistema di sicurezza e i programmi di accesso previa comunicazione del Responsabile.

Eventuali usi impropri degli archivi devono essere segnalati dagli Incaricati al responsabile del trattamento.

Per i casi di esternalizzazione del servizio, il raccordo e operato d'intesa con il soggetto esterno, tramite atti formali, secondo le regole stabilite nel successivo articolo 16.

L'elenco e i relativi trattamenti dei dati sensibili effettuati dal Comune di Manfredonia sono stati individuati in apposito regolamento in corso di approvazione; l'elenco contenente i nominativi dei soggetti che vi operano è in ogni caso allegato sotto la lettera A al presente documento.

La comunicazione dei dati all'interno della struttura comunale, per ragioni d'ufficio, non è soggetta a limitazioni particolari, salvo quelle espressamente previste dalle leggi e regolamenti.

Art. 10
(Risorse informatiche del Comune di Manfredonia. Analisi della vulnerabilità)

Il Servizio Sistemi Informativi del Comune di Manfredonia, con lo scopo di classificare beni gestiti e valutarne le minacce e la vulnerabilità ha eseguito il censimento delle banche dati e delle postazioni di lavoro presenti nell'Ente, utilizzando un modello descrittivo in cui si analizzano tutte le caratteristiche principali delle diverse procedure relative all'erogazione dei servizi informatici del Comune.

La sicurezza informatica dei dati può essere fatta derivare dalla corretta e accurata gestione delle seguenti quattro tipologie di risorse:

1. Risorse hardware

   Si tratta delle componenti fisiche del Sistema Informativo, server, personal computer, stampanti, disk drive. Sulle postazioni acquisite tramite il Servizio Sistemi Informativi, viene richiesto un periodo di garanzia in loco di tre anni dal momento dell'acquisto.

   Vulnerabilità: occorre garantire assistenza oltre tale periodo mediante un contratto con ditte specializzate.

2. Risorse software (Sistemi Operativi, Software Applicativo, Banche Dati)

   L'elenco di tutte le risorse software, ridefinito e aggiornato è presente presso il Servizio Sistemi Informativi e Statistica.

I software in uso dagli uffici del Comune di Manfredonia sono riconducibili a tre categorie:

1. software proprietario, cioè sviluppato dai tecnici del Servizio Sistemi Informativi e Statistica;

2. software acquistato sul mercato;

3. software ricevuto da altri Enti.

I software proprietari sono procedure sviluppate con i prodotti di Microsoft Office, utilizzate in rete su diverse postazioni di lavoro (gestione del protocollo, gestione determinazioni, deliberazioni di Giunta, gestione flussi documentali, software di controllo dati).

Per quanto riguarda il software acquistato, il Comune di Manfredonia si affida a ditte fornitrici di livello nazionale, in grado garantire la buona qualità soprattutto in relazione agli aggiornamenti normativi.

In ogni caso viene assicurato il *back-up* o salvataggio dei dati, procedura attraverso la quale viene periodicamente effettuata una copia di tutti i dati presenti nel sistema su supporti da conservare separatamente. In caso di guasto hardware dei dischi è quindi possibile "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo back-up. Il back-up viene effettuato periodicamente, in base alle necessita e la gestione dei supporti è tale da scongiurare i disastri derivanti da cause fisiche (incendi, distruzione di locali, ecc.).

Vulnerabilità: In molti casi i supporti di salvataggio vengono conservati nella stessa stanza in cui risiedono i Personal Computer. In questo modo, in caso di furto o incendio dei locali non sarebbe più possibile recuperare gli archivi. E' nelle intenzioni dell'amministratore utilizzare un'apposita cassaforte ignifuga presso i locali del Tesoriere, ovvero sistemi alternativi in grado di assicurare comunque il salvataggio dei dati.

3. Risorse logistiche (locali, linee di comunicazione)

   Si ritiene utile richiamare l'attenzione sui locali in cui sono collocati i server. Attualmente viene garantita la chiusura degli ingressi ai locali dei server, e, più in generale, alla chiusura degli accessi agli edifici comunali.

   Vulnerabilità: occorre aumentare la protezione dei locali che ospitano i server, collocare porte blindate e cancelli alle finestre.

4. Risorse professionali (dipendenti, professionisti esterni, collaboratori)

   Il personale dipendente è stato nominato incaricato del trattamento dei dati.

   Per i casi di personale esterno autorizzato all'accesso, inclusi i tecnici che si occupano di assistenza ai software gestionali, Responsabili del trattamento dei dati del Comune di Manfredonia nominano gli stessi Incaricati al trattamento dei dati relativi alle banche dati a cui viene permesso l'accesso.

   Vulnerabilità: talvolta l'accesso alle banche dati da parte di esterni può sfuggire al Responsabile del trattamento dati. Occorre, tramite apposita formazione, fare in modo che gli incaricati facciano osservare sempre le regole di accesso ai dati da parte di terzi.

Art. 11
(Architettura di rete del Comune di Manfredonia)

Nel 2004 è stato realizzato il cablaggio dei seguenti locali del Comune di Manfredonia:

1. Sede centrale - Palazzo di Città
2. Ufficio Tecnico - Palazzina ex Bozzelli
3. Via Orto Sdanga - Servizi Demografici, Annona e Servizi alle Imprese
4. Servizi Sociali - via Torre dell'Abate

per un totale di 276 postazioni di lavoro.

Nel 2005 sono stati cablati i seguenti locali del Comune di Manfredonia:

5. Comando dei Vigili - Largo G. Mondelli
6. Biblioteche civiche - Corso Manfredi
7. Pubblica Istruzione - Via Maddalena

Nel 2004 e nel 2005 le Circoscrizioni comunali sono state dotate di linee Internet ADSL, tramite le quali accedono ai dati presenti sul server dei Servizi Demografici, per mezzo di credenziali. L'utilizzo di tale sistema web in modalità protetta, consente l'accesso ai dati in tempo reale da parte di utenti autorizzati e permette di non avere dati da proteggere presso le sedi delle Circoscrizioni.

Buona parte dei servizi comunali è attualmente collegata in rete per consentire la condivisione degli archivi e delle risorse e soprattutto l'accesso alla rete Internet tramite linee ADSL con costi fissi per l'Ente.

Ogni apparecchio di collegamento alla rete esterna (router), è protetto da sistemi di sicurezza (firewall) interni o esterni, che consentono anche la registrazione dei siti a cui si è fatto accesso dalle postazioni di lavoro. Il controllo degli accessi ha l'obiettivo di garantire che la rete sia utilizzata esclusivamente dall'utenza autorizzata e nelle modalità definite dai profili di abilitazione.

La maggior parte delle postazione e dotata di password per l'accesso al computer, e di password per l'accesso agli archivi in rete.

La gestione delle password, dove è possibile, viene delegata all'utente; in caso contrario, il Servizio Sistemi Informativi assegna all'utente un codice individuale di accesso al servizio.

In particolare la procedura di gestione dei Servizi Demografici prevede in automatico la modifica obbligatoria delle password ogni sei mesi.

Art. 12
(analisi dei rischi che incombono sui dati)

L'approccio alla sicurezza deve avvenire in una logica di prevenzione piuttosto che in una logica di gestione delle emergenze o di semplice controllo/vigilanza.

L'architettura per rispondere alle esigenze di sicurezza è costituita dai seguenti elementi fondamentali:

- le politiche dell'organizzazione;
- gli strumenti organizzativi e tecnologici;
- gli atteggiamenti individuali.

Un sistema di gestione della sicurezza delle informazioni efficiente ed efficace permette all'organizzazione di:

- implementare politiche e procedure di primaria importanza, mantenersi aggiornata su nuove minacce e vulnerabilità e prenderle in considerazione in modo sistematico;
- sapere quando politiche di sicurezza e procedure non sono implementate in tempo utile per prevenire danni;
- trattare incidenti e perdite in ottica di prevenzione e di miglioramento continuo dal sistema.

Tra le risorse da tutelare rientrano:

- dati digitali, documenti cartacei, flussi informativi;
- computer e reti;
- il personale;
- edifici e uffici.

In relazione all'organizzazione del Comune di Manfredonia si elencano i principali rischi che incombono sui dati:

- assenza di infrastrutture tecniche di sicurezza (inferriate, sistemi di allarme perimetrale, sorveglianza, etc);
- non adeguato controllo degli accessi alle postazioni di lavoro e/o agli uffici;
- assenza di inventario delle risorse;

- password troppo semplici;
- assenza di aggiornamento periodico delle password;
- assenza di firewall interni presso alcune sedi periferiche.

Art. 13

(Misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità)

Rischio	Misure da adottare
assenza di infrastrutture tecniche di sicurezza (inferriate, sistemi di allarme perimetrale, sorveglianza, etc.)	Presso le sedi che ospitano i server dati, sii propone di installare: - una porta blindata presso il centro stella di Piazza del Popolo; - una porta blindata e inferriate alle finestre presso il centro stella di Via Orto Sdanga;
Chiusura dei contenitori	Occorre cambiare la chiusura degli armadi e dei cassetti presso vari uffici del Comune.
Non adeguato controllo degli accessi alle postazioni di lavoro e/o agli uffici	- Registrare gli accessi ai locali, soprattutto quando avvengono su dati sensibili oltre l'orario di lavoro, utilizzando il modello dell'allegato E. - Individuare i depositari delle chiavi di apertura dei locali comunali
Assenza di inventario delle risorse	Occorre istituire un inventario unico delle risorse informatiche al fine di tenere sotto controllo tutto il Sistema informativo comunale. Per ogni risorsa deve essere dichiarato: - Il settore e il servizio a cui è assegnata la risorsa; - Il responsabile della risorsa; - Le autorizzazioni di accesso e di utilizzo della risorsa.
Password troppo semplici	Spesso le password di accesso alle postazioni informatiche vengono scelte dal personale sono semplici, facilmente individuabili e spesso note a più persone.
Assistenza di aggiornamento periodico delle password	Le password di accesso alla rete e alle procedure devono essere cambiate ogni sei

	mesi.
Assenza di un contratto di manutenzione dei personal computer	Al fine di prevenire i problemi dovuti al malfunzionamento hardware occorre stipulare un contratto di manutenzione dei PC, che includa anche la verifica periodica dei Sistemi Operativi e degli Antivirus presenti sulle singole macchine.

Art. 14
(Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento)

Per assicurare la continuità dei servizi devono essere valutate le strategie di ripristino più opportune dei dati.

A tal fine, ogni Responsabile individua uno o più addetti al salvataggio dei dati di propria competenza e stabilisce la frequenza di salvataggio anche in base al tipo di aggiornamento dei dati.

Non è possibile effettuare il salvataggio dei dati su strumenti tipo pen-drive, ma esclusivamente su cd riscrivibili. Il salvataggio deve essere eseguito una volta alla settimana obbligatoriamente con le seguenti modalità: con il masterizzatore si esegue la copia dei dati dal disco fisso; dopo la verifica dell'avvenuta procedura di salvataggio il CD opportunamente etichettato viene rimosso e custodito nel luogo prescelto; la settimana successiva si dovrà introdurre un secondo CD per la registrazione che si alternerà con l'altro per l'attuazione del salvataggio programmato; deve essere prevista una verifica mensile della suddetta procedura da parte dei Responsabili del trattamento dei dati; inoltre, semestralmente i due CD devono essere rinnovati e la sostituzione dei CD avverrà uno alla volta;

Il supporto di salvataggio deve essere custodito in siti diversi da quello in cui si trova la banca dati, al fine di garantire il ripristino dei dati anche in caso di attacchi alla sede in cui essi si trovano.

Deve essere conservata in sede separata anche copia della procedura di gestione dei dati al fine di ripristinare immediatamente gli stessi all'interno della procedura stessa.

Art. 15
(Interventi formativi degli incaricati del trattamento)

Il Responsabile del trattamento dati, insieme al Responsabile della sicurezza esegue interventi di formazione nei confronti degli incaricati al fine di renderli edotti circa:

- i rischi che incombono sui dati;

- le misure disponibili per prevenire eventi dannosi;

- i profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;

- le responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Presso ciascun Settore sarà effettuata e documentata la formazione del Personale durante il trimestre successivo all'approvazione del presente atto e sarà comunque garantita periodicamente in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati.

Art. 16
(Trattamenti affidati all'esterno)

Nel rispetto della normativa emessa dal *Garante*, la comunicazione, la diffusione e il trasferimento dei dati personali sono effettuati solo se previsti da norme di legge, di regolamento, o che risultino comunque necessari per lo svolgimento di funzioni istituzionali e per essi si applicano le disposizioni di cui all'articolo 19 del *Codice in materia di protezione di dati personali.*

Il Comune di Manfredonia, in relazione ai trattamenti di dati personali affidati all'esterno della struttura comunale, adotta i seguenti criteri per garantire le misure minime di sicurezza.

a) il Titolare dei dati del Comune di Manfredonia nomina "Responsabile della Banca dati" il Legale rappresentante o il Dirigente dell'Ente che richiede l'accesso dati da parte, al quale vengono consegnate personalmente le credenziali di accesso e tenuto a sua volta a nominare ufficialmente i propri incaricati (allegato B);

b) il Responsabile della banca dati del Comune di Manfredonia nomina direttamente *Incaricato del trattamento* il personale che esegue materialmente l'accesso ai dati al quale vengono consegnate personalmente le credenziali di accesso (allegato C);

In tutti i casi tutti i fornitori e i prestatori d'opera che eseguono lavori per i quali vengono a conoscenza di dati personali, sensibili e giudiziari del Comune di Manfredonia, sono tenuti ad osservare le disposizioni della comunicazione.

Per le banche dati per le quali è tecnicamente possibile, è consentito il trattamento tramite accesso telematico da parte di Strutture Sanitarie pubbliche o altri enti pubblici, ferma restando la formalizzazione tramite gli allegati B e C.

Nel caso di accesso telematico ai dati da parte di Autorità di pubblica sicurezza o delle forze di Polizia, il trattamento avviene in conformità del Titolo II – "Trattamenti da parte di forze di Polizia" del *Codice in materia di protezione di dati personali*.

ALLEGATO A

Elenco trattamenti relativi a dati sensibili e giudiziari del Comune di Manfredonia

Nome	*Tipo dati*
Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune	*Sensibili*
Santoro Domenico	Inserimento e modifica dati
Storace Mattia Siponta	Inserimento e modifica dati
La Forgia Gaetano	Inserimento e modifica dati
De Palma Sante	Inserimento e modifica dati
Anagrafe popolazione residente popolazione residente all'estero (AIRE)	*Sensibili*
Di Candia Michele Ciro	Inserimento e modifica dati
Vitulano Matteo	Inserimento e modifica dati
Mangano Rita	Inserimento e modifica dati
Cotrufo Filomena	Consultazione dati
Gramazio Raffaele (LSU)	Consultazione dati
Troiano Margherita (LSU)	Consultazione dati
Cinque Matteo	Consultazione dati
Trotta Domenico	Consultazione dati
Saracino Maria Teresa	Consultazione dati
Rinaldi Giuseppe Luigi	Consultazione dati
Castigliego Antonio	Consultazione dati
Vitale Maria	Consultazione dati
Ufficio Servizi Sociali	Consultazione dati
Giardino Davide	Consultazione dati
Della Torre Alfredo Giuseppe	Consultazione dati
Accarino Pasquina	Consultazione dati
Palma Pasquina	Consultazione dati
Iacoviello Andrea	Consultazione dati
Fano Margherita	Inserimento e modifica dati
Palumbo Antonino	Inserimento e modifica dati
Conoscitore Giuseppina	Consultazione dati
Santoro Silvestro	Consultazione dati
Marasco Domenico	Consultazione dati
Caputo Pietro	Consultazione dati
Gatta Aldo Antonio	Consultazione dati
Robustella Maria Giacinta	Consultazione dati
Totaro Michele	Consultazione dati
Altavilla Fausta (LSU)	Consultazione dati

Spano Giuseppe	Consultazione dati
Angelillis Libera (LSU)	Consultazione dati
Leone Michelina (LSU)	Consultazione dati
Gelsomino Maria (LSU)	Consultazione dati
Amoroso Ilaria (LSU)	Consultazione dati
Totano Matteo (LSU)	Consultazione dati
Ufficio Tributi	Consultazione dati
Vigili Urbani	Consultazione dati

Registri di stato civile	*Sensibili*
Accarino Pasquina	Inserimento e modifica dati
Della Torre Alfredo Giuseppe	Inserimento e modifica dati
Cotrufo Filomena	Inserimento e modifica dati
Totano Michele	Inserimento e modifica dati
Rinaldi Giuseppe Luigi	Inserimento e modifica dati
Di Candia Michele Ciro	Consultazione dati
Mangano Rita	Consultazione dati
Vitulano Matteo	Consultazione dati
Vitale Maria	Consultazione dati
Robustella Maria Giacinta	Consultazione dati
Gatta Aldo Antonio	Consultazione dati
Marasco Domenico	Consultazione dati
Conoscitore Giuseppina	Consultazione dati
Iacoviello Andrea	Consultazione dati
Caputo Pietro	Consultazione dati
Palma Caterina	Consultazione dati
Cinque Matteo	Consultazione dati
Trotta Domenico	Consultazione dati
Saracino Maria Teresa	Consultazione dati
Giardino Davide	Consultazione dati
Castigliego Antonio	Consultazione dati
Fano Margherita	Inserimento e modifica dati
Palumbo Antonio	Inserimento e modifica dati

Elettorato attivo e passivo	*Sensibili*
Robustella Maria Giacinta	Modifica e inserimento
Caputo Pietro	Modifica e inserimento
Gatta Aldo Antonio	Modifica e inserimento
Marasco Domenico	Modifica e inserimento
Di Candia Michele Ciro	Consultazione dati
Mangano Rita	Consultazione dati
Vitulano Matteo	Consultazione dati
Vitale Maria	Consultazione dati
Iacoviello Andrea	Consultazione dati
Santoro Silvestro	Consultazione dati

Conoscitore Giuseppina	Consultazione dati
Saracino Maria Teresa	Consultazione dati
Accarino Pasquina	Consultazione dati
Totaro Michele	Consultazione dati
Castigliego Antonio	Consultazione dati
Giardino Davide	Consultazione dati
Trotta Domenico	Consultazione dati
Cinque Matteo	Consultazione dati
Palma Caterina	Consultazione dati
Cotrufo Filomena	Consultazione dati
Rinaldi Giuseppe Luigi	Consultazione dati
Della Torre Alfredo Giuseppe	Consultazione dati
Fano Margherita	Inserimento e modifica dati
Palumbo Antonio	Inserimento e modifica dati
Personale autorizzato con straordinario elettorale	Consultazione dati

Albo degli scrutatori e dei presidenti di seggio	*Sensibili*
Robustella Maria Giacinta	Modifica e inserimento
Gatta Aldo Antonio	Modifica e inserimento
Caputo Pietro	Modifica e inserimento
Marasco Domenico	Modifica e inserimento
Fano Margherita	Modifica e inserimento
Palumbo Antonio	Modifica e inserimento

Elenco dei giudici popolari	*Sensibili*
Robustella Maria Giacinta	Modifica e inserimento
Marasco Domenico	Modifica e inserimento
Caputo Pietro	Modifica e inserimento
Gatta Aldo Antonio	Modifica e inserimento
Palumbo Antonio	Inserimento e modifica dati

Obiettori di coscienza	*Sensibili*
Santoro Silvestro	Inserimento e modifica dati
Conoscitore Giuseppina	Inserimento e modifica dati

Liste di leva e dei registri matricolari	*Sensibili*
Santoro Silvestro	Inserimento e modifica dati
Conoscitore Giuseppina	Inserimento e modifica dati

Assistenza domiciliare anziani e disabili	*Sensibili*
Imperato Maddalena	Inserimento e modifica dati
Dentellato Angelo Claudio	A conoscenza verbale dei dati

Gramazio Maria Filippa	Inserimento e modifica dati
D'Antuono Angela	Consultazione dati
Rinaldi Francesco	A conoscenza verbale dei dati
Trotta Giuseppe	A conoscenza verbale dei dati
Murgo Lucia (LSU)	Consultazione dati
Grilli Libera Maria G.	Inserimento e modifica dati
Angelillis Maria (LSU)	Consultazione dati
Ricucci Daniela (LSU)	Consultazione dati
Vairo Antonio	A conoscenza verbale dei dati
Talamo Antonio	A conoscenza verbale dei dati

Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, etc.	*Sensibili*
Imperato Maddalena	Inserimento e modifica dati
Angelillis Maria (LSU)	Consultazione dati
Grilli Libera Maria G.	Inserimento e modifica dati
Gramazio Maria Filippa	Inserimento e modifica dati
Ricucci Daniela (LSU)	Consultazione dati
Marinaro Salvatore	Consultazione dati
D'Antuono Angela	Consultazione dati
Russo Sante	Consultazione dati
Murgo Lucia (LSU)	Consultazione dati

Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale	*Sensibili*
Imperato Maddalena	Inserimento e modifica dati
Simone Rosa Pina	Inserimento e modifica dati
Grilli Libera MAria G.	Inserimento e modifica dati
De Cristofaro Eleonora	Inserimento e modifica dati
Luriola Michela (LSU)	Consultazione dati
Rinaldi Giovanni §(ass. sociale incaricato)	Inserimento e modifica dati
Valente Gabriele Pio	Inserimento e modifica dati
Russo Sante	Consultazione dati
D'Antuono Angela	Consultazione dati
Marinaro Salvatore	Consultazione dati
Angelillis Maria (LSU)	Consultazione dati
Ricucci Daniela (LSU)	Consultazione dati
Murgo Lucia (LSU)	Consultazione dati
Gramazio Maria Filippa	Inserimento e modifica dati

Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo	*Sensibili*

(per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico

Imperato Maddalena	Inserimento e modifica dati
Murgo Lucia (LSU)	Consultazione dati
Luriola Michela (LSU)	Consultazione dati
Russo Sante	Consultazione dati
Grilli Libera Maria G.	Inserimento e modifica dati
Gramazio Maria Filippa	Inserimento e modifica dati
De Cristofaro Eleonora	Inserimento e modifica dati
Simone Rosa Pina	Inserimento e modifica dati
Rinaldi Giovanni (ass. sociale incaricato)	Inserimento e modifica dati
D'Antuono Angela	Consultazione dati
Valente Gabriele Pio	Inserimento e modifica dati
Ricucci Daniela (LSU)	Consultazione dati
Angelillis Maria (LSU)	Consultazione dati
Marinaro Salvatore	Consultazione dati

Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, ecc.)	*Sensibili*

Imperato Maddalena	Consultazione dati
Gramazio Maria Filippa	Inserimento e modifica dati
Grilli Libera Maria G.	Inserimento e modifica dati
D'Antuono Angela	Consultazione dati
De Cristofaro Eleonora	Inserimento e modifica dati
Simone Rosa Pina	Inserimento e modifica dati
Rinaldi Giuseppe (ass. sociale incaricato)	Inserimento e modifica dati
Russo Sante	Consultazione dati
Lauriola Michela (LSU)	Consultazione dati
Murgo Lucia (LSU)	Consultazione dati
Ricucci Daniela (LSU)	Consultazione dati
Marinaro Salvatore	Consultazione dati
Angelillis MAria (LSU)	Consultazione dati

Attività relativa alla prevenzione ed al soggetto alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione)	*Sensibili*

Rinaldi Giovanni (ass. sociale incaricato)	Inserimento e modifica dati
Murgo Lucia (LSU)	Consultazione dati
Ricucci Daniela (LSU)	Consultazione dati
Angelillis Maria (LSU)	Consultazione dati
Marinaro Salvatore	Consultazione dati

D'Antuono Angela	Consultazione dati
De Cristofaro Eleonora	Inserimento e modifica dati
Valente Gabriele Pio	Inserimento e modifica dati
Simone Rosa Pina	Inserimento e modifica dati
Lauriola Michela (LSU)	Consultazione dati
Russo Sante	Consultazione dati

Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affido e di adozione dei minori	*Sensibili*
Imperato Maddalena	Consultazione dati
Russo Sante	Consultazione dati
Rinaldi Giovanni (ass. sociale incaricato)	Inserimento e modifica dati
Simone Rosa Pina	Inserimento e modifica dati
D'Antuono Angela	Consultazione dati
Marinaro Salvatore	Consultazione dati
Angelillis Maria (LSU)	Consultazione dati
Ricucci Daniela (LSU)	Consultazione dati
Lauriola Michela (LSU)	Consultazione dati
Murgo Lucia (LSU)	Consultazione dati
De Cristofaro Eleonora	Inserimento e modifica dati

Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) e all'assistenza sanitaria obbligatoria (A.S.O.)	*Sensibili*
Salvemini Silvana	A conoscenza verbale dei dati
Remore Antonio	A conoscenza verbale dei dati
Personale presente in reperibilità	A conoscenza verbale dei dati
Personale Polizia Locale	A conoscenza verbale dei dati

Attività relative alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario	*Sensibili*
Imperato Maddalena	Inserimento e modifica dati
Gramazio Maria Filippa	Inserimento e modifica dati
Palumbo Matteo	Inserimento e modifica dati
D'Antuono Angela	Inserimento e modifica dati
Valente Gabriele Pio	Inserimento e modifica dati
Rinaldi Giovanni (ass. sociale incaricato)	Inserimento e modifica dati
De Cristofaro Eleonora	Inserimento e modifica dati
Grilli Libera Maria G.	Inserimento e modifica dati
Simone Rosa Pina	Inserimento e modifica dati

Attività relativa alle gestione degli asili nido Comunali e dei servizi per l'infanzia e delle scuole Materne elementari e medie	*Sensibili*
Imperato Maddalena	Inserimento e modifica dati
De Cristofaro Eleonora	Inserimento e modifica dati
Simone Rosa Pina	Inserimento e modifica dati
Rinaldi Giovanni (ass. sociale incaricato)	Inserimento e modifica dati
D'Antuono Angela	Inserimento e modifica dati
Angelillis Maria (LSU)	Consultazione dati
Ricucci Daniela (LSU)	Consultazione dati
Murgo Lucia (LSU)	Consultazione dati
Lauriola Michela (LSU)	Consultazione dati
Attività relativa all'infortunistica stradale	*Sensibili*
Fusco Mario	Inserimento e modifica dati
Ciuffreda Michele	Inserimento e modifica dati
Guerra Vincenzo	Inserimento e modifica dati
Gestione delle procedure sanzionatorie	*Sensibili*
Fusco Mario	Inserimento e modifica dati
Attività di polizia annonaria, commerciale ed amministrativa	*Sensibili*
Artuso Pasquale	Inserimento e modifica dati
Falcone Giuseppe	Inserimento e modifica dati
Angelillis Antonio	Inserimento e modifica dati
Castrignano Tommaso	Inserimento e modifica dati
Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria	*Sensibili*
Spagnuolo Nicola	Inserimento e modifica dati
Stelluti Giuseppe	Inserimento e modifica dati
Gravinese Renato	Inserimento e modifica dati
Vero Francesco Paolo	Inserimento e modifica dati
Marasco Francesco Paolo	Inserimento e modifica dati
Attività relativa al rilascio di permessi per invalidi	*Sensibili*
Fusco Mario	Inserimento e modifica dati
Borgia Giosafatte	Inserimento e modifica dati

Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza	*Sensibili*
Angelillis Antonio	Inserimento e modifica dati
Falcone Giuseppe	Inserimento e modifica dati
Artuso Pasquale	Inserimento e modifica dati
Castrignano Tommaso	Inserimento e modifica dati
Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione	*Sensibili*
Totaro Teresa Siponta	Inserimento e modifica dati
Troiano Raffale V.	Inserimento e modifica dati
Attività politica, di indirizzo di controllo, sindacato ispettivo e documentazione dell'attività istituzionale degli organi comunali	*Sensibili*
Di Candia Paolo (coll.re Sindaco)	Inserimento e modifica dati
Cotrufo Michele (LSU)	Inserimento e modifica dati
Lapiccirella Domenico	Inserimento e modifica dati
Gare di appalto e affidamenti	*Sensibili*
Iacoviello Sistiana	A conoscenza dei dati ricevuti
Castigliego Vittorio	A conoscenza dei dati ricevuti
Vaira Libera Maria	A conoscenza dei dati ricevuti
Operazioni di Polizia Giudiziaria	*Sensibili*
Fusco Mario	Inserimento e modifica dati
Spagnuolo Nicola	Inserimento e modifica dati
Esposto Gregorio	Inserimento e modifica dati
Denunce infortuni sul lavoro	*Sensibili*
Ardò Luigi Andrea	Inserimento e modifica dati
Damiano Carmela	Inserimento e modifica dati
Castigliego Matteo	Inserimento e modifica dati
Li Bergoli Michele	Inserimento e modifica dati
Visite medico collegiali	*Sensibili*
Gentile Gennaro	Inserimento e modifica dati

Ciuffreda Libero	Inserimento e modifica dati
Trattenute sindacali	*Sensibili*
Ardò Luigi Andrea	Inserimento e modifica dati
Damiano Carmela	Inserimento e modifica dati
Li Bergoli Michele	Inserimento e modifica dati
Castigliego Matteo	Inserimento e modifica dati
ICI – agevolazioni tariffarie	*Sensibili*
Pacilli Vincenza	Inserimento e modifica dati
Leone Mattia	Inserimento e modifica dati
Feltri Matteo Carmine	Inserimento e modifica dati
Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi relativi all'eliminazione di barriere architettoniche in edifici privati	*Sensibili*
Imperato Maddalena	Inserimento e modifica dati
Russo Sante	Inserimento e modifica dati
Marinaro Salvatore	Consultazione dati
Lauriola Michela (LSU)	Consultazione dati
Ricucci Daniela (LSU)	Consultazione dati
Angelillis Maria)LSU)	Consultazione dati
Murgo Lucia (LSU)	Consultazione dati

ALLEGATO B

AOO: Comune di Manfredonia
UOR: _____
Protocollo n. _____
Data: __/__/____
CAT./CLASSE: ___/__

OGGETTO: NOMINA A RESPONSABILE DEL TRATTAMENTOI DATI

In esecuzione del "indicare il provvedimento e la motivazione di affidamento dei dati all'esterno", il destinatario della presente è autorizzato a svolgere operazioni di trattamento di dati personali per conto del Comune di Manfredonia sulla banca dati "_____", aggiornata alla data _____, ed è tenuto a rispettare ed osservare tutte le norme del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali", nonché ogni altra istruzione impartita in calce alla presente o in successive comunicazioni da parte dell'Amministrazione stessa.

In caso di inadempimento, il destinatario della presente comunicazione sarà considerato *Responsabile* ai sensi del *"Codice in materia di protezione di dati personali", nei confronti del Titolare*, relativamente alle operazioni effettuate senza la diligenza dovuta in esecuzione delle istruzioni ricevute, ferme in ogni caso le proprie responsabilità civili e penali in caso di abuso dei dati personali di cui sia venuto a conoscenza in esecuzione del rapporto instaurato con l'amministrazione Comunale.

In caso il destinatario si avvalga di incaricati o collaboratori, è obbligato a nominarli ufficialmente incaricati del trattamento dei dati ed a renderli edotti delle norme operative generali, fermo restando che in ogni caso essi si intendono operare sotto la sua diretta ed esclusiva responsabilità.

In caso di cessazione del trattamento il destinatario dovrà distruggere i dati personali provvedendo alle necessarie formalità, inclusa la consegna degli stessi al Comune in formato elettronico e su supporto cartaceo.

IL TITOLARE

_____

ALLEGATO C

AOO: Comune di Manfredonia
UOR: _____ sig. <nome incaricato del trattamento>
Protocollo n. _____
Data: __/__/____
CAT./CLASSE: ___/__

OGGETTO: ASSEGNAZIONE PASSWORD PER ACCESSO ALLA DATI "_____". NOMINA A INCARICATO DEL TRATTAMENTO.

In riferimento all'oggetto la S.V. è autorizzata all'accesso della banca dati "_____" del Comune di Manfredonia e al trattamento per le finalità istituzionali assumendo il ruolo di "Incaricato al trattamento dei dati".

A tal fine si ricorda che, per lo svolgimento dei propri compiti, bisognerà attenersi alle seguenti disposizioni e a quanto previsto dal *Codice in materia di protezione dei dati personali:*

1. In relazione alle indicate finalità, il trattamento dei dati avviene anche mediante strumenti informatici e telematici, tramite computer, protetti da password di cui ne è vietata la diffusione e la pubblicità.

2. Il trattamento di dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti.

3. Le stampe effettuate, relative a dati personali devono essere conservate in archivi ad accesso controllato chiusi.

4. I dati sensibili eventualmente trattati, ai sensi dell'articolo 20 del Decreto Legislativo 30 giugno 2003, n. 196 devono essere conservati in buste chiuse e in armadi chiusi.

5. E' fatto divieto di consentire a persone non autorizzate l'accesso alla banca dati in oggetto.

La conoscenza dei dati personali da parte Sua non è considerata comunicazione né violazione della privacy.

Con la presente, in allegato si consegna il supporto contenente la banca dati in oggetto, aggiornata alla data _____, secondo le modalità concordate.

IL RESPONSABILE DEL TRATTAMENTO DATI

_____

ALLEGATO D

AOO: Comune di Manfredonia
UOR: _____
Protocollo n. _____
Data: __/__/____
CAT./CLASSE: ___/__

sig. <Indirizzato ad almeno due incaricati per banca dati>

OGGETTO: NOMINA A INCARICATO DEL SALVATAGGIO DEI DATI

Il destinatario della presente è nominato incaricato del salvataggio della banca dati "_____".

Non è possibile effettuare il salvataggio dei dati su strumenti tipo pen-drive, ma esclusivamente su CD riscrivibili.

Il salvataggio deve essere eseguito una volta alla settimana obbligatoriamente con le seguenti modalità: con il masterizzatore si esegue la copia dei dati dal disco fisso; dopo la verifica dell'avvenuta procedura di salvataggio il CD opportunamente etichettato viene rimosso e custodito nel luogo prescelto; la settimana successiva si dovrà introdurre un secondo CD per la registrazione che si alternerà con l'altro per l'attuazione del salvataggio programmato.

Semestralmente i due CD devono essere rinnovati e la sostituzione dei CD avverrà uno alla volta.

In caso di assenza prolungata l'incaricato dovrà informare il Responsabile affinché sia sempre garantito il salvataggio.

IL RESPONSABILE DEL TRATTAMENTO DATI

_____

REGISTRO TRATTAMENTO DATI SENSIBILI O GIUDIZIARI EXTRA ORARIO

Ufficio _____

Data e ora	Operatore	Attività	Motivazione	Tipo di dati trattati (sensibili o giudiziari)	Firma dell'operatore

IL SEGRETARIO GENERALE IL PRESIDENTE

_____ _____

ATTESTAZIONE

Si attesta che il presente atto:

1. su analoga attestazione del messo comunale è stato pubblicato in copia all'Albo Pretorio dal **04 APRILE 2006** al **19 APRILE 2006** e contro di essa ……. sono state presentate opposizioni.

2. è stato trasmesso in elenco ai Capi Gruppo Consiliari con nota n. _____ del _____.

3. è stato trasmesso al Prefetto di Foggia con nota n. _____ del _____.

4. è stato trasmesso in data _____ ai seguenti uffici:

   - _____;
   - _____;
   - _____;

5. è divenuto esecutivo il **04 APRILE 2006** ai sensi di legge.

Lì, ……

IL SEGRETARIO GENERALE

…….