Comune di Gessate

PROVINCIA DI MILANO
PIAZZA DEL MUNICIPIO, 1
TEL. 02/959299.1 – FAX 02/95382853

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N. 35 del 31-03-2010

COPIA

Oggetto:	APPROVAZIONE DOCUMENTO PROGRAMMATICO PER LA SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI ALL'INTERNO DELL'ENTE.

L'anno duemiladieci, addì trentuno del mese di marzo alle ore 18:30, presso la sede municipale, appositamente convocati, si sono riuniti gli assessori comunali, per deliberare sulle proposte all'ordine del giorno della seduta.

Dei componenti la Giunta Comunale di questo Comune:

LEONI MARIO GIUSEPPE	P
ROMEO FRANCESCO	P
TAUSCHECK ROBERTO	P
PIROZZI GIOVANNI	P
BALCONI ANTONIO	A

ne risultano presenti n. 4 e assenti n. 1.

Assume la presidenza il Sindaco LEONI MARIO GIUSEPPE e partecipa il Segretario Comunale LIVERANI MINZONI MASSIMO.

Il Presidente, accertato il numero legale per poter deliberare validamente, invita la Giunta Comunale ad assumere le proprie determinazioni sulla proposta di deliberazione indicata in oggetto.

Deliberazione G.C. n.35 del 31/03/2010.

OGGETTO: Aggiornamento Documento Programmatico per la Sicurezza nel trattamento dei dati personali all'interno dell'Ente.

LA GIUNTA COMUNALE

Richiamata la propria deliberazione n.217 del 10/12/2004, esecutiva, con la quale è stato adottato il "Documento Programmatico per la Sicurezza per il trattamento dei dati personali all'interno dell'Ente";

Preso atto che a decorrere dall'anno 2005 è stato affidato alla società Halley Lombardia s.n.c. il servizio di aggiornamento annuale del Documento predetto;

Sentita la Società Halley Lombardia s.n.c. la quale, a conclusione della fase 1 e della fase 2 del 'progetto privacy', si è resa disponibile alla manutenzione del Documento Programmatico per la Sicurezza nel trattamento dei dati personali all'interno dell'Ente anche per l'anno corrente;

Dato atto che, per la parte tecnica, la revisione del documento è stata condotta con l'ausilio della Società Bit & Bit, s.n.c. che offre il servizio di assistenza e manutenzione dell'infrastruttura informatica del Comune di Gessate;

Ritenuto l'allegato "Documento Programmatico per la Sicurezza per il trattamento dei dati personali all'interno dell'Ente" così come aggiornato, meritevole di approvazione;

Visto l'art.3, co.4 del Regolamento sull'Ordinamento degli Uffici e dei Servizi,

Visto l'art.41 dello Statuto Comunale rubricato "Le funzioni e le competenze della Giunta Comunale";

Visto il D.Lgs. n.196/2003 "Codice in materia di protezione dei dati personali";

Acquisiti gli allegati pareri resi ai sensi dell'art. 49, co.1, D.Lgs. n.267/2000 (T.U.E.L.) e dell'art.50, co.2, dello Statuto Comunale;

Con voto unanime;

D E L I B E R A

1. Di approvare l'allegato documento programmatico per la sicurezza e per il trattamento dei dati personali all'interno dell'Ente, così come aggiornato e revisionato con l'ausilio della predetta Società Bit & Bit, s.n.c. che offre il servizio di assistenza e manutenzione dell'infrastruttura informatica del Comune di Gessate;

2. Di prendere atto che il presente provvedimento non comporta spesa, idoneo impegno di spesa verrà assunto successivamente dal Responsabile del Servizio interessato, come indicato nell'allegato parere;

3. Di demandare al Responsabile del Servizio interessato l'adozione di tutti gli atti conseguenti necessari all'applicazione del Documento Programmatico predetto;

4. Di trasmette il presente provvedimento, contestualmente all'affissione all'albo, ai Capigruppo Consiliari;

Allegati:

- Pareri art.49 TUEL
- Documento programmatico per la sicurezza e per il trattamento dei dati personali all'interno dell'Ente

Il presente verbale è stato letto, approvato e sottoscritto.

Il Presidente
F.to Dr. LEONI MARIO GIUSEPPE

Il Segretario Comunale
F.to LIVERANI MINZONI MASSIMO

CERTIFICATO DI PUBBLICAZIONE E COMUNICAZIONE

La presente deliberazione è stata affissa all'Albo Pretorio di questo Comune in data odierna e vi resterà in pubblicazione per 15 giorni consecutivi.
Si dà atto che del presente verbale viene data comunicazione in data odierna ai capigruppo consiliari, ai sensi dell'art. 125 del D.Lgs. n.267/2000.

Gessate, 01-06-2010

La Responsabile Servizio Affari Generali
F.to D.ssa FACCHINETTI ROSAMARINA

CERTIFICATO DI ESECUTIVITA'

La presente deliberazione è stata pubblicata dal 01-06-2010 al 15-06-2010, con/senza opposizioni ed è diventata esecutiva in data 11-06-2010 ai sensi dell'Art. 134, co.3, del D.Lgs. n.267/2000.

Gessate,

La Responsabile Servizio Affari Generali
F.to D.ssa FACCHINETTI ROSAMARINA

Copia conforme all'originale

Gessate, 01-06-2010

La Responsabile Servizio Affari Generali
D.ssa FACCHINETTI ROSAMARINA

Rosamarina Facchinetti

Comune di Gessate
Provincia di Milano
comune.gessate@legalmail.it

P.zza Municipio 1-20060 Gessate (MI)
Tel. 02.959299.200 -Fax 02.95382853
P.I. 00973680150

P702
M002
Rev.1/10

Allegato "A" alla deliberazione di Giunta Comunale n. 35 **del** 31 MAR 2010

FOGLIO PARERI

(ART. 49 – I COMMA – DEL D.L.VO N. 267/2000 E ARTICOLO 34 DEL VIGENTE REGOLAMENTO DI ORGANIZZAZIONE DEGLI UFFICI E DEI SERVIZI DEL COMUNE DI GESSATE)

OGGETTO: APPROVAZIONE DOCUMENTO PROGRAMMATICO PER LA SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI ALL'INTERNO DELL'ENTE

Sul presente atto esprimo PARERE FAVOREVOLE di regolarità tecnica.

Gessate, 31 MAR 2010

Il Responsabile del Servizio Affari Generali
D.ssa Rosamarina Facchinetti
Rosamarina Facchinetti

Sul presente atto esprimo PARERE FAVOREVOLE di regolarità contabile dell'atto.

☒ Il provvedimento non comporta spesa o diminuzione di entrata. L'impegno di spesa verrà assunto con successiva Determinazione a cura dal Responsabile del Servizio Affari Gererali.

☐ La spesa viene imputata ai seguenti capitoli:

Numero Impegno	Codice Intervento	Capitolo	Importo Euro

del Bilancio ……. che presenta la necessaria disponibilità e copertura finanziaria.

☐ L'entrata viene introitata al seguente capitolo:

Numero Accertamento	Codice Risorsa	Capitolo	Importo Euro

del Bilancio ……

Gessate, 31 MAR2010

Il Responsabile del Servizio Finanziario
Rag. Renata Capitanio

Sul presente atto esprimo PARERE FAVOREVOLE di conformità all'ordinamento giuridico.

Gessate, 31 MAR 2010

Il Segretario Comunale
Dr. Massimo Liverani Minzoni

ALLEGATO ALLA DELIBERAZIONE
G.C. n. 35 del 31 MAR 2010

Comune di Gessate
Provincia di Milano

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI ALL'INTERNO DELL'ENTE

(art. 34 e regola 19 dell'allegato B del dlgs 30.06.2003, n. 196)

INDICE

Premessa

Con Decreto Legislativo 30 giugno 2003 n. 196 è stato approvato il "Codice in materia di protezione dei dati personali" che ha praticamente abrogato la legge 31 dicembre 1996 n. 675 e successive modifiche e integrazioni.

Il nuovo codice reca una serie di disposizioni a tutela della protezione dei dati personali trattati sia dagli enti pubblici che dagli enti privati e garantisce che il trattamento degli stessi si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Nella normativa si precisa altresì che il trattamento dei dati personali viene disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati nonché per l'adempimento degli obblighi da parte del titolare del trattamento. Tutti i sistemi informativi ed i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando i fini perseguiti nei diversi casi possono essere conseguiti con dati anonimi od opportune modalità che consentano di identificare l'interessato solo in caso di necessità.

Il codice disciplina il trattamento dei dati personali anche detenuti all'estero effettuati da chi è stabilito nel territorio dello stato o comunque in un luogo soggetto alla sovranità dello stato; pertanto l'ente locale è soggetto alle disposizioni ivi contenute.

Prima di addentrarsi nello specifico è opportuno richiamare alcune definizioni fornite dalla vigente normativa e necessarie ai fini del presente documento quali:

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 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;

d) "**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;

e) "**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;

f) "**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;

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

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

i) "**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;

l) "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

L'ente nel momento in cui raccoglie i dati deve effettuare una informativa scritta o orale in merito a:

a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7 del D.Lgs. n. 196/2003;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 del codice e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

Negli articoli 18 e seguenti del D.Lgs. n.196/2003 vengono individuate le regole particolari a cui devono attenersi i soggetti pubblici nel trattamento dei dati con esclusione degli enti pubblici economici. Si precisa innanzitutto che qualunque trattamento di dati personali da parte dei soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali; inoltre il trattamento di dati diversi da quelli sensibili e giudiziari è consentito, salvo quanto sopra, anche in mancanza di una norma di legge o di regolamento che lo prevede espressamente.

La comunicazione di dati da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2 del codice, e non è stata adottata la diversa determinazione ivi indicata.

La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Una norma di notevole importanza per l'attività dell'ente locale è quella contenuta nell'art. 20 del D.Lgs 196/2003 ove si afferma che il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge che specifichi i tipi di dati che possono essere trattati e di operazioni eseguibili nonché le finalità di rilevante interesse pubblico perseguite.

Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare, che dovrà essere adottato da ogni singolo ente, in conformità al parere espresso dal Garante, ai sensi dell'articolo 154, comma 1, lettera g) del D.Lgs 196/03.

Il codice per la protezione di dati personali pone particolare attenzione alla sicurezza dei dati e dei sistemi ed in particolare alle misure minime di sicurezza che devono essere adottate dagli enti volte ad assicurare un livello minimo di protezione dei dati personali.

In merito alle misure di sicurezza in generale il codice dispone che i dati personali oggetto di trattamento sono custoditi e controllati in modo da ridurre al minimo il rischio di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'articolo 34 del codice invece disciplina il trattamento dei dati con l'ausilio di strumenti elettronici e lo ritiene possibile solo se vengono adottate, nei modi previsti dal disciplinare tecnico di cui all'allegato B del D.Lgs 196/2003, le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Stante le regole suddette riveste una notevole importanza il documento programmatico sulla sicurezza che deve essere aggiornato annualmente entro il 31 marzo.

Approssimandosi la scadenza si rende necessario dare attuazione alla normativa predisponendo il documento che segue.

Nella predisposizione di tale atto sono state prese in considerazione la struttura organizzativa dell'ente, la dotazione organica, il sistema informativo, i rischi che incombono sui dati e tutta una serie di documenti che emergeranno nel corso della stesura.
Per quanto attiene in particolare il sistema informativo è stato svolto un censimento dello stesso ponendo particolare attenzione alla tipologia di hardware presente nell'ente e per ogni macchina ai programmi installati; tale lavoro è riportato nell'allegato "audit analitico del sistema informatico (hardware e software)" parte integrante del presente DPS.

In conclusione di questa premessa è opportuno ricordare che:

- il Comune di Gessate ha redatto un Documento Programmatico per la Sicurezza dei Dati D.Lgs. 196/03 approvato per la prima volta con atto di Giunta Comunale n. 217 del 10 Dicembre 2004 poi aggiornato ed approvato annualmente, così come previsto dalla legislazione vigente;
- i dipendenti del Comune di Gessate hanno partecipato ad un "Corso di formazione privacy e sicurezza dati" tenuto dalla ditta Frareg s.r.l. in data ..... ed è in programma .....

Elenco dei trattamenti dei dati personali
(Regola 19.1)

L' ente nell'espletamento della propria attività istituzionale tratta tutta una serie di dati, personali, anche giudiziari e sensibili gestiti a volte in forma diretta ed a volta in forma indiretta tramite ditte, società, cooperative ecc.

Dall'esame della situazione interna all'ente, dalle attività svolte e dal confronto con le categorie di dati contenute anche nelle tabelle degli schemi di notificazione dati predisposte dal Garante per la notificazione emerge che l'ente svolge i seguenti trattamenti:

Tabella 1.1 Elenco dei trattamenti: informazioni di base

Id del trattamento	Descrizione sintetica	Natura dei dati trattati		Area / Servizio di riferimento	Altre strutture o aree (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
		Sens.	Giudiz.			
1	Dati idonei a rivelare la vita sessuale	SI		Servizio Socio Culturale		Server, Personal computer e archivi cartacei
2	Dati idonei a rivelare lo stato di disabilità	SI		Servizio Socio Culturale	Servizio Polizia Locale, Servizio Affari Generali, Servizi Demografici, , Servizio Finanziario, Coop. PIANETA AZZURRO – Corsico Coop. BATHOR – Vigevano Consorzio FARSI PROSSIMO – Milano Cooperativa PUNTO D'INCONTRO – Cassano d'Adda (fraz. Groppello d'Adda) Cooperativa sociale LA FRATERNITÀ - Cernusco sul Naviglio Cooperativa Sociale INSIEME A R.L. – Melzo Cooperativa Sociale PAPA GIOVANNI XXIII – Rimini Cooperativa Sociale LA FRATERNITÀ – Rimini Cooperativa Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda) Associazione VOS – Sezione di Gessate	Server, Personal computer e archivi cartacei
3	Dati idonei a rivelare sieropositività	SI		Servizio Socio Culturale		Server, Personal computer e archivi cartacei
4	Dati idonei a rivelare malattie infettive e diffusive	SI		Servizio Socio Culturale	Servizio Polizia Locale	Server, Personal computer e archivi cartacei
5	Dati idonei a rivelare malattie mentali	SI		Servizio Socio Culturale	Servizio Polizia Locale, Servizio Affari Generali, Servizi Demografici, , Coop. BATHOR – Vigevano Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda)	Server, Personal computer e archivi cartacei

					Associazione VOS – Sezione di Gessate D.d.P., Scuola, Comune Gorgonzola C.D.D.	
6	Dati idonei a rivelare lo stato di salute	SI		Servizio Socio Culturale, Servizio Affari Generali, Servizi Demografici,	Coop. PIANETA AZZURRO – Corsico Coop. BATHOR – Vigevano Consorzio FARSI PROSSIMO – Milano Cooperativa PUNTO D'INCONTRO – Cassano d'Adda (fraz. Groppello d'Adda) Cooperativa sociale LA FRATERNITÀ – Cernusco sul Naviglio Cooperativa Sociale INSIEME A R.L. – Melzo Cooperativa Sociale PAPA GIOVANNI XXIII – Rimini Cooperativa Sociale LA FRATERNITÀ – Rimini Cooperativa Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda) Associazione VOS – Sezione di Gessate Scuola, Comune Gorgonzola C.D.D.	Server, Personal computer e archivi cartacei
7	Dati relativi a prescrizioni farmaceutiche e cliniche	SI		Servizio Socio Culturale, Servizio Affari Generali, Servizi Demografici,	Coop. PIANETA AZZURRO – Corsico Coop. BATHOR – Vigevano Consorzio FARSI PROSSIMO – Milano Cooperativa PUNTO D'INCONTRO – Cassano d'Adda (fraz. Groppello d'Adda) Cooperativa sociale LA FRATERNITÀ - Cernusco sul Naviglio Cooperativa Sociale INSIEME A R.L. – Melzo Cooperativa Sociale PAPA GIOVANNI XXIII – Rimini Cooperativa Sociale LA FRATERNITÀ – Rimini Cooperativa Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda) Associazione VOS – Sezione di Gessate Scuola, Comune Gorgonzola C.D.D.	Server, Personal computer e archivi cartacei
8	Dati relativi ad esiti diagnostici e programmi terapeutici	SI		Servizio Socio Culturale, Servizio Affari Generali, Servizi Demografici,	Coop. PIANETA AZZURRO – Corsico Coop. BATHOR – Vigevano Consorzio FARSI PROSSIMO – Milano Cooperativa PUNTO D'INCONTRO – Cassano d'Adda (fraz. Groppello d'Adda) Cooperativa sociale LA FRATERNITÀ - Cernusco sul Naviglio	Server, Personal computer e archivi cartacei

					Cooperativa Sociale INSIEME A R.L. – Melzo Cooperativa Sociale PAPA GIOVANNI XXIII – Rimini Cooperativa Sociale LA FRATERNITÀ – Rimini Cooperativa Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda) Associazione VOS – Sezione di Gessate Scuola, Comune Gorgonzola C.D.D.	
9	Dati relativi all'utilizzo di particolari ausili protesici	SI		Servizio Socio Culturale, Servizio Affari Generali, Servizi Demografici,	Coop. PIANETA AZZURRO – Corsico Coop. BATHOR – Vigevano Consorzio FARSI PROSSIMO – Milano Cooperativa PUNTO D'INCONTRO – Cassano d'Adda (fraz. Groppello d'Adda) Cooperativa sociale LA FRATERNITÀ - Cernusco sul Naviglio Cooperativa Sociale INSIEME A R.L. – Melzo Cooperativa Sociale PAPA GIOVANNI XXIII – Rimini Cooperativa Sociale LA FRATERNITÀ – Rimini Cooperativa Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda) Associazione VOS – Sezione di Gessate Scuola, Comune Gorgonzola C.D.D.	Server, Personal computer e archivi cartacei
10	Dati relativi alla prenotazione di esami clinici e visite specialistiche	SI		Servizio Socio Culturale, Servizio Affari Generali, Servizi Demografici,	Coop. PIANETA AZZURRO – Corsico Coop. BATHOR – Vigevano Consorzio FARSI PROSSIMO – Milano Cooperativa PUNTO D'INCONTRO – Cassano d'Adda (fraz. Groppello d'Adda) Cooperativa sociale LA FRATERNITÀ - Cernusco sul Naviglio Cooperativa Sociale INSIEME A R.L. – Melzo Cooperativa Sociale PAPA GIOVANNI XXIII – Rimini Cooperativa Sociale LA FRATERNITÀ – Rimini Cooperativa Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda) Associazione VOS – Sezione di Gessate Scuola, Comune Gorgonzola C.D.D.	Server, Personal computer e archivi cartacei
11	Dati idonei a rivelare AIDS conclamato	SI		Servizio Socio Culturale	Coop. PIANETA AZZURRO – Corsico	Server, Personal computer e

					Coop. BATHOR – Vigevano Consorzio FARSI PROSSIMO – Milano Cooperativa PUNTO D'INCONTRO – Cassano d'Adda (fraz. Groppello d'Adda) Cooperativa sociale LA FRATERNITÀ - Cernusco sul Naviglio Cooperativa Sociale INSIEME A R.L. – Melzo Cooperativa Sociale PAPA GIOVANNI XXIII – Rimini Cooperativa Sociale LA FRATERNITÀ – Rimini Cooperativa Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda) Associazione VOS – Sezione di Gessate	archivi cartacei
12	Dati giudiziari		SI	Servizio Polizia Locale, Servizio Lavori Pubblici, Servizio Edilizia-Urbanistica/Tutela Ambientale, Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale, Servizio Finanziario	Polizia Locale Ufficio di Piano Cooperativa Bathor, Cooperativa Punto d'Incontro, Scuola	Server, Personal computer e archivi cartacei
13	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche			Servizio Affari Generali, Servizi Demografici,	Coop. PIANETA AZZURRO – Corsico Coop. BATHOR – Vigevano Consorzio FARSI PROSSIMO – Milano Cooperativa PUNTO D'INCONTRO – Cassano d'Adda (fraz. Groppello d'Adda) Cooperativa sociale LA FRATERNITÀ - Cernusco sul Naviglio Cooperativa Sociale INSIEME A R.L. – Melzo Cooperativa Sociale PAPA GIOVANNI XXIII – Rimini Cooperativa Sociale LA FRATERNITÀ – Rimini Cooperativa Cooperativa Sociale LA GOCCIA - Cassano d'Adda (fraz. Groppello d'Adda) Associazione VOS – Sezione di Gessate Scuola, Comune Gorgonzola C.D.D.	Server, Personal computer e archivi cartacei
14	Dati idonei a rivelare convinzioni di altro genere (diverse da religiose o filosofiche)	SI		Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale	Ufficio di Piano Sodexo	Server, Personal computer e archivi cartacei

15	Dati idonei a rivelare gusti, preferenze, abitudini di vita o di consumo			Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale	Sodexo Italia S.p.A.	Server, Personal computer e archivi cartacei
16	Dati idonei a rivelare l'adesione a partiti	SI		Servizio Affari Generali, Servizi Demografici,	Servizio Finanziario	Server, Personal computer e archivi cartacei
17	Dati idonei a rivelare l'adesione a sindacati	SI		Servizio Affari Generali, Servizi Demografici,	Servizio Finanziario	Server, Personal computer e archivi cartacei
18	Dati idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	SI		Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale, Servizio Finanziario		Server, Personal computer e archivi cartacei
19	Dati idonei a rivelare le convinzioni filosofiche	SI		Servizio Socio Culturale		Server, Personal computer e archivi cartacei
20	Dati idonei a rivelare le convinzioni religiose	SI		Servizio Socio Culturale		Server, Personal computer e archivi cartacei
21	Dati idonei a rivelare le opinioni politiche	SI		Servizio Socio Culturale, Servizio Affari Generali, Servizi Demografici,		Server, Personal computer e archivi cartacei
22	Dati idonei a rivelare lo stato matrimoniale o di famiglia			Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale		Server, Personal computer e archivi cartacei
23	Dati idonei a rivelare l'origine nazionale	SI		Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale		Server, Personal computer e archivi cartacei
24	Dati idonei a rivelare l'origine razziale ed etnica	SI		Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale		Server, Personal computer e archivi cartacei
25	Dati relativi a comportamenti illeciti o fraudolenti		SI	Servizio Polizia Locale, Servizio Socio Culturale	Servizio Affari Generali, Servizi Demografici, , Servizio Lavori Pubblici, Servizio Edilizia e Ambiente, Polizia Locale	Server, Personal computer e archivi cartacei
26	Dati relativi ad altri provvedimenti o procedimenti giudiziari		SI	Servizio Polizia Locale, Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale, Servizio Lavori Pubblici, Servizio Edilizia-Urbanistica/Tutela Ambientale	Polizia Locale	Server, Personal computer e archivi cartacei

27	Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili		SI	Servizio Polizia Locale, Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale, Servizio Finanziario	Polizia Locale	Server, Personal computer e archivi cartacei
28	Dati relativi al comportamento debitorio			Servizio Finanziario, Servizio Lavori Pubblici, Servizio Edilizia-Urbanistica/Tutela Ambientale, Servizio Affari Generali, Servizi Demografici,		Server, Personal computer e archivi cartacei
29	Dati relativi al grado di istruzione o di cultura			Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale		Server, Personal computer e archivi cartacei
30	Dati relativi alle pregresse esperienze professionali			Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale, Servizio Finanziario		Server, Personal computer e archivi cartacei
31	Dati relativi allo svolgimento di attività economiche e altre informazioni commerciali (es. fatturato, bilanci, aspetti economici, finanziari, organizzativi, produttivi, industriali, commerciali, imprenditoriali)			Servizio Affari Generali, Servizi Demografici, , Servizio Socio Culturale, Servizio Finanziario, Servizio Lavori Pubblici, Servizio Edilizia-Urbanistica/Tutela Ambientale		Server, Personal computer e archivi cartacei
32	Dati idonei a rivelare l'appartenenza a categorie protette	SI		Servizio Affari Generali, Servizio Socio Culturale		Server, Personal computer e archivi cartacei
33	Dati idonei a rivelare lo stato di gravidanza	SI		Servizio Affari Generali, Servizi Demografici, Servizio Socio Culturale	Ufficio di Piano	Server, Personal computer e archivi cartacei
34	Dati relativi ad eventuali controversie con precedenti datori di lavoro		SI	Servizio Affari Generali		Server, Personal computer e archivi cartacei
35	Gestione archivio comunale	SI	SI	Servizio Affari Generali		Server, Personal computer e archivi cartacei
36	Gestione albo pretorio e notifiche		SI	Servizio Polizia Locale		Server, Personal computer e archivi cartacei
37	Gestione anagrafe della popolazione residente in Italia e all'estero e relativi adempimenti	SI	SI	Servizi Demografici		Server, Personal computer e archivi cartacei

38	Gestione stato civile della popolazione residente e relativi adempimenti	SI	SI	Servizi Demografici		Server, Personal computer e archivi cartacei
39	Gestione schedario elettorale e relativi fascicoli	SI		Servizi Demografici		Server, Personal computer e archivi cartacei
40	Aggiornamento elenco giudici popolari		SI	Servizi Demografici		Server, Personal computer e archivi cartacei
41	Gestione del personale dipendente dell'ente e relativi adempimenti	SI	SI	Servizio Finanziario, Servizio Affari Generali	Studio GARZON –Porto Mantovano	Server, Personal computer e archivi cartacei
42	Gestione assicurazioni dell'ente	SI	SI	Servizio Affari Generali		Server, Personal computer e archivi cartacei
43	Gestione procedimenti di spesa e di entrata			Servizio Finanziario	Revisore dei conti	Server, Personal computer e archivi cartacei
44	Riscossioni di tributi e imposte diverse			Servizio Finanziario	CEM S.p.A. Duomo G.P.A. Tecnologia & Territorio	Server, Personal computer e archivi cartacei
45	Gestione economato, acquisto beni e servizi e appalti di lavori pubblici e relativi adempimenti conseguenti (es. espropri, trattative bonarie)		SI	Servizio Finanziario, Servizio Lavori Pubblici, Servizio Edilizia-Urbanistica/ Tutela Ambientale, Servizio Polizia Locale, Servizio Affari Generali, Servizi Demografici, Servizio Socio Culturale		Server, Personal computer e archivi cartacei
46	Gestione procedimenti in materia di polizia amministrativa (autorizzazione, licenze, permessi, ecc.)		SI	Servizio Polizia Locale		Server, Personal computer e archivi cartacei
47	Procedimenti connessi all'applicazione del codice della strada (contravvenzioni, infrazioni, rilevazioni incidenti stradali)	SI	SI	Servizio Polizia Locale		Server, Personal computer e archivi cartacei
48	Acquisizione denuncie d'infortunio	SI		Servizio Polizia Locale		Server, Personal computer e archivi cartacei
49	Gestione servizi assistenziali a favore della popolazione bisognosa (anziani, minori in difficoltà, portatori di handicap, ecc.) ivi compresa l'erogazione di contributi	SI	SI	Servizio Socio Culturale, Servizio Finanziario		Server, Personal computer e archivi cartacei
50	Gestione asilo nido e adempimenti conseguenti	SI		Servizio Socio Culturale	Coop. PIANETA AZZURRO – Corsico Scuola Materna STEFANO LATTUADA	Server, Personal computer e archivi cartacei
51	Attività inerenti la biblioteca comunale	SI		Servizio Socio Culturale	Sistema bibliotecario di Melzo	Server, Personal computer e archivi cartacei
52	Gestione pratiche per il rilascio concessioni edilizie o autorizzazioni			Servizio Lavori Pubblici, Servizio Edilizia-Urbanistica/Tut		Server, Personal computer e archivi cartacei

				ela Ambientale		

Il trattamento dei dati riportati nella tabella suddetta è rivolto al perseguimento degli obiettivi dell'ente e si riferisce alle attività d'ufficio svolte dallo stesso quali ad esempio la gestione del personale, l'acquisto di beni e servizi, la gestione dei fornitori e dei clienti ecc..
Le categorie di persone a cui i dati trattati si riferiscono sono i cittadini che intrattengono rapporti con l'ente, i fornitori, dipendenti, collaboratori, utenti dei servizi erogati dall'ente ecc

Tutti i trattamenti indicati nella tabella 1.1 sono registrati in banche dati memorizzate in un server e sono gestiti dagli incaricati del trattamento attraverso personal computer collegati in rete, le copie dei dati sono salvate giornalmente su dischi USB che vengono conservati in un armadio blindato posto nell'ufficio Ragioneria, lontano dalle Sale Macchine ubicate presso l'ufficio Tecnico situato al secondo piano della sede comunale.

Tutti gli armadi e i classificatori contenenti dati personali sono ad accesso selezionato e muniti di serratura con chiavi.
Ogni atto e documento contenente dati personali, sensibili e giudiziari è conservato a cura di ciascun Incaricato in appositi contenitori (armadi e classificatori) muniti di serratura, come previsto nella lettera di nomina ad Incaricato.

I dati cartacei sono posti nelle seguenti sedi comunali in appositi armadi chiusi a chiave:

- P.za Municipio, 1

Distribuzione dei compiti e delle responsabilità
(Regola 19.2)

Categoria Giuridica	Nr. Dipendenti a Tempo Indeterminato	Nr. Dipendenti a Tempo Determinato	Nr. Dipendenti Part Time
B1	3	0	0
B3	6	0	2
C	15	0	1
D1	6	0	1
D3	1	0	0
Dirigenti	0	0	0
totale	31	0	4

- Segretario Comunale in convenzione con il Comune di Ronco Briantino;
- Servizio Polizia Locale – per brevi periodi estivi e per alcune funzioni - in convenzione con altri Comuni.

La struttura organizzativa dell'ente è divisa nelle seguenti aree / servizi:

- Servizio Affari Generali
- Servizi Demografici
- Servizio Edilizia, Urbanistica e Tutela Ambientale
- Servizio Finanziario
- Servizio Lavori Pubblici
- Servizio Polizia Locale
- Servizio Socio Culturale

Per quanto attiene la privacy sono state effettuate, da parte del titolare le seguenti nomine per gli incaricati e per i responsabili del trattamento; con decreti sindacali stati nominati responsabili del trattamento il Vicesindaco e i Responsabili dei servizi; con lettera sono stati nominati incaricati del trattamento i dipendenti dell'ente.
Con appositi provvedimenti sono stati e verranno nominati responsabili del trattamento le imprese esterne che trattano dati per l'Ente.

Ditta	Trattamento	Inizio mandato	Fine mandato
Banca di Credito Cooperativo di Carugate	Servizio di tesoreria comunale		
Bernini Daniela	Riordino archivi		
Bit@Bit	Fornitura ed assistenza hardware		
CEM S.p.A.	Riscossione ruoli TARSU		
BATHOR	Assistenza domiciliare minori e servizio psicologico		
Consorzio Farsi Prossimo	SAD Anziani e disabili		
Esatri S.p.A.	Tributi Vari		

H.C.M. Cooperativa Sociale	Servizio infermieristico		
Halley Informatica di Ciccolini G. & C. snc - Matelica	Fornitura ed assistenza software		
Halley Lombardia di Monti, Molteni & C. snc – Cantù	Redazione DPS		
IDRA SPA	Gestione servizio acquedotto		
Maggioli SPA	Gestione multe, cessioni di fabbricato e ospitalità stranieri		
Polisportiva Gessate	Gestione impianti sportivi		
Massimo Giudici	Revisore dei conti		
Scuola Materna STEFANO LATTUADA	Gestione micronido		
Sistema bibliotecario comunale – Melzo	Prestiti bibliotecari		
Sodexo Italia S.p.A.	Gestione servizi amministrativi refezione		
Studio GARZON	Gestione stipendi		
Studio R.L. SRL	Medico del lavoro		
Tecnologia & Territorio	Accertamenti ICI, bollettazione e rendicontazione ICI		
E.On Rete Orobica	Gestione servizio gas		
Ufficio di Piano – Gorgonzola	Affidi/Adozioni Servizi Sociali		
Zovi Paola	Trasporto documenti Enti Pubblici Milano		

In base alle necessità organizzative interne all'ente i procedimenti indicati nella tabella 1.1 sono effettuati dalle diverse strutture come emerge nella tabella che segue:

Tabella 2.1 Aree preposte ai trattamenti

Area Funzionale	**Responsabile**	**Trattamenti operati dall'area (rif. identificativo del trattamento in tab. 1.1)**	**Descrizioni dei compiti e delle responsabilità della struttura**
Servizi Demografici, Servizio Affari Generali	Dr. Massimo Liverani Minzoni D.ssa Rosamarina Facchinetti	6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 21, 22, 23, 24, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 45	La struttura nel trattamento dei dati citati svolge diverse attività quali l'acquisizione e il caricamento dei dati, la consultazione, la comunicazione a terzi ecc..; in merito alla manutenzione tecnica dei programmi, alla gestione tecnico

			operativa dei database quali salvataggi, ripristini ecc... ,si avvale della collaborazione del responsabile dei backup
Servizio Edilizia-Urbanistica/Tutela Ambientale	Geom. Gatti Christian	12, 26, 28, 31, 45, 52	La struttura nel trattamento dei dati citati svolge diverse attività quali l'acquisizione e il caricamento dei dati, la consultazione, la comunicazione a terzi ecc..; in merito alla manutenzione tecnica dei programmi, alla gestione tecnico operativa dei database quali salvataggi, ripristini ecc... ,si avvale della collaborazione del responsabile dei backup
Servizio Finanziario	Rag. Capitanio Renata	12, 18, 27, 28, 30, 31, 41, 43, 44, 45, 49	La struttura nel trattamento dei dati citati svolge diverse attività quali l'acquisizione e il caricamento dei dati, la consultazione, la comunicazione a terzi ecc..; in merito alla manutenzione tecnica dei programmi, alla gestione tecnico operativa dei database quali salvataggi, ripristini ecc... ,si avvale della collaborazione del responsabile dei backup
Servizio Lavori Pubblici	Dr. Massimo Liverani Minzoni	12, 26, 28, 31, 45, 52	La struttura nel trattamento dei dati citati svolge diverse attività quali l'acquisizione e il caricamento dei dati, la consultazione, la comunicazione a terzi ecc..; in merito alla manutenzione tecnica dei programmi, alla gestione tecnico operativa dei database

			quali salvataggi, ripristini ecc... ,si avvale della collaborazione del responsabile dei backup
Servizio Polizia Locale	Comandante Frigerio Walter	12, 25, 26, 27, 45, 46, 47, 48	La struttura nel trattamento dei dati citati svolge diverse attività quali l'acquisizione e il caricamento dei dati, la consultazione, la comunicazione a terzi ecc..; in merito alla manutenzione tecnica dei programmi, alla gestione tecnico operativa dei database quali salvataggi, ripristini ecc... ,si avvale della collaborazione del responsabile dei backup
Servizio Socio Culturale	D.ssa Sancini Nadia	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 45, 49, 50, 51	La struttura nel trattamento dei dati citati svolge diverse attività quali l'acquisizione e il caricamento dei dati, la consultazione, la comunicazione a terzi ecc..; in merito alla manutenzione tecnica dei programmi, alla gestione tecnico operativa dei database quali salvataggi, ripristini ecc... ,si avvale della collaborazione del responsabile dei backup

Per quanto attiene i compiti svolti dalla diverse strutture in merito ai trattamenti operati dalle stesse si precisa che vengono svolte attività di acquisizione e caricamento dei dati, modifica, cancellazione e consultazione comunicazioni a terzi, gestione tecnico operativa della base dati con relativi salvataggi e ripristini.

Analisi dei rischi che incombono sui dati
(Regola 19.3)

Gli uffici comunali sono attrezzati con dispositivi antincendio atti a prevenire il danneggiarsi delle attrezzature, in conformità alle vigenti disposizioni di Legge.
Gli stabili comunali sono protetti da porte chiuse a chiave, da un sistema di allarme per gli uffici dell'anagrafe. Le chiavi di accesso ai locali sono custodite dal personale incaricato (solo alcuni dipendenti hanno le chiavi).
Il sistema informativo del Comune di Gessate è costituito dalla presenza di N.35 computer client in rete tra di loro, N. 0 computer non in rete e N.3 computer portatili.
Ad ogni utente viene assegnata una User-ID (definita dal livello di accesso che si sta utilizzando) e una password standard.
Ogni utente modifica la password al primo accesso. La password è di almeno 8 caratteri alfanumerici e non è riconducibile alla persona. Nei casi in cui il software applicativo non consente il cambio della password da parte dell'utente, è il responsabile del CED che provvede a fornirne una secondo le regole sopra descritte.

Nonostante tutti questi accorgimenti i rischi che incombono sui dati sono notevoli e si rende pertanto necessario valutare le possibili conseguenze, la gravità e porli in relazione con misure consone.
Dall'esame della concreta situazione dell'ente si possono presumere i rischi riportati nella seguente tabella in cui la voce gravità stimata viene graduata da 0 a 10, dove 0 è una bassa gravità e 10 una alta gravità.

Tabella 3.1 Analisi dei rischi

Evento	**Impatto sulla sicurezza dai dati**		**Rif. Misure d'azione**
	Descrizione	**Gravità stimata**	
Comportamenti degli operatori			
Furto o smarrimento di credenziali di autenticazione	Consente l'accesso alle banche dati ad estranei	3	Sottolineare l'importanza delle credenziali a tutti i dipendenti evidenziando la necessità di una immediata comunicazione dell'evento furto o smarrimento al responsabile designato per l'adozione dei provvedimenti necessari, incaricare il responsabile delle password di depositare in cassaforte, in busta chiusa sigillata, tutte le password
Carenza di consapevolezza, disattenzione o incuria	La carenza di conoscenze di carattere informatico/amministrativo nonché la superficialità nell'utilizzo degli strumenti può arrecare al sistema ingenti danni, a volte	7	Svolgere un'intensa attività di formazione al personale per renderlo edotto dei possibili rischi e danni, adottare giornalmente la copia di salvataggio dei dati e depositarla a cura del responsabile designato in cassaforte

	anche irreparabili		
Comportamenti sleali o fraudolenti	L'utilizzo su pc dell'ufficio di software non autorizzati dal responsabile costituisce un comportamento sleale che può anche arrecare danni alle banche dati dell'ente; l'utilizzo per fini propri di banche dati o software dell'ente costituisce comportamento fraudolento	7	Informare il personale attraverso un'apposita circolare firmata per ricevuta da ogni dipendente, Installare appositi software che impediscano ai dipendenti l'utilizzo di programmi non autorizzati dal responsabile, attribuire la custodia dei software e relative licenze al responsabile designato ammonendolo che qualsiasi abuso o uso non autorizzato sarà di sua responsabilità, Disattivare eventuali account di posta elettronica personali e impedire che ne vengano configurati di nuovi
Errore materiale	E' un episodio che può verificarsi al quale bisogna dare la dovuta attenzione ma non sopravvalutarlo anche se da questo possono derivare danni al trattamento dei dati	3	Svolgere un'intensa attività formativa al personale e mettere a disposizione dello stesso un referente per la soluzione dei problemi che possono verificarsi nell'espletamento del lavoro
Comportamenti degli operatori			
Azione di virus informatici o di programmi suscettibili di recare danno	L'ingresso di virus nel sistema può creare ingenti danni al trattamento dei dati.; tale problematica si può anche verificare qualora vengano utilizzati programmi non autorizzati	7	-Installazione antivirus tenuti costantemente aggiornati con sistemi automatizzati, Attribuire al responsabile designato il compito di fare l'aggiornamento, Impedire l'installazione di programmi suscettibili di recare danno alla rete
Spamming o altre tecniche di sabotaggio	La ricezione di e-mail da parte di soggetti non istituzionali arreca problemi al trattamento dei dati e satura inutilmente la casella e-mail con il rischio di importare virus nascosti	4	Adozione di programmi antispamming, Formazione del personale per renderlo edotto sull'uso corretto della posta elettronica
Spooffing: falsificazione di e-mail	Con appositi	3	Adozione di programmi

	software informatici gli hackers sono in grado di inviare documenti utilizzando il vostro indirizzo e-mail		antispooffing
Tampering: alterazione di dati durante la transazione	Con appositi software gli hacker sono in grado di intercettare il messaggio e-mail e variarne il contenuto	3	Adozione di programmi di crittografia, Introdurre o sviluppare l'uso della firma digitale
Denial of service: saturazione di una rete con pacchetti ICMP	Con appositi software gli hacker possono inviare migliaia di pacchetti al secondo verso la linea adsl dell'ente saturandola e rendendola inutilizzabile	3	Disabilitare la risposta al ping sul router o sul firewall
Malfunzionamento, indisponibilità o degrado degli strumenti	Il malfunzionamento delle apparecchiature così come apparecchiature degradate possono recare danni al trattamento dei dati o non garantire il pieno rispetto della normativa del trattamento degli stessi. L'indisponibilità di una macchina può provocare che, utilizzando altre macchine con la stessa user e password, altri soggetti vengano a conoscenza di una certa banca dati.	6	Assicurare la manutenzione ordinaria attraverso appositi contratti manutentivi, Provvedere alla sostituzione delle apparecchiature al fine di prevenire il degrado o l'indisponibilità degli strumenti
Accessi esterni non autorizzati	Qualsiasi forma di intrusione dall'esterno al sistema informatico arreca	4	Adozione di sistemi firewall, con relativo aggiornamento periodico

	danni alle banche dati creando notevoli disagi e problemi a tutta la struttura		
Eventi relativi al contesto fisico ambientale			
Accessi non autorizzati ai locali da parte di soggetti esterni	L'accesso da parte degli estranei agli uffici comunali può consentire agli stessi di venire a conoscenza di una serie di dati anche personali relativi a pratiche trattate dai singoli uffici.	5	Nel caso si renda necessario abbandonare l'ufficio lo stesso deve essere chiuso a chiave al fine di evitare l'ingresso di estranei; nel caso in cui non sia possibile tutti gli strumenti elettronici devono essere dotati di password di screen saver con un tempo di intervento massimo di 10 minuti e gli armadi e i cassetti contenenti i documenti chiusi a chiave
Asportazione e furto di strumenti contenenti dati (ad esempio pc, notebook, palmari, cellulari ecc..)	Il furto di materiale è un evento che può verificarsi e pertanto è necessario adottare tutti gli accorgimenti possibili al fine di evitare che possano essere utilizzati i dati contenuti negli strumenti sia cartacei che informatici	5	Tutte le apparecchiature informatiche ed in generale tutti gli strumenti contenenti i dati devono essere protetti con sistemi di allarme; in particolar modo le apparecchiature informatiche devono essere dotate di password e di sistemi di crittografia, oltre che ove necessario codici PIN, I pc portatili dovranno essere dotati di cavetto di sicurezza e comunque non devono mai essere lasciati incustoditi dai loro consegnatari. Quindi si rende necessario nel provvedimento di assegnazione del portatile al consegnatario specificare le incombenze e le responsabilità alle quali è sottoposto.
Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Il verificarsi di eventi distruttivi potrebbe comportare la perdita completa dei dati; è necessario perciò, nonostante ci si auspichi che non capitino mai, pensare a sistemi che consentano di subire le minori conseguenze	2	Adozione di una cassaforte ignifuga dove riporre i salvataggi quotidiani, Dividere il rischio di smarrimento e perdita dati, portando in un locale idoneo esterno alla struttura una copia dei dati con cadenza settimanale (ad esempio cassetta di sicurezza in banca)

	possibili		
Guasto ai sistemi complementari (impianto elettrico, climatizzazione)	Non avere una linea elettrica dedicata può comportare un funzionamento anomalo del sistema informatico e la conseguente perdita di dati; così pure il surriscaldamento delle macchine costituisce un grosso rischio per il corretto funzionamento del sistema	3	Per un corretto funzionamento del sistema è necessario che lo stesso sia dotato di una apposita linea elettrica dedicata nonché di gruppi di continuità che assicurino quantomeno, in caso di guasti alla linea elettrica o interruzioni di somministrazione dell'energia, il salvataggio dei dati. Tutti i server devono essere posti in locali appositamente climatizzati al fine di consentirne il corretto funzionamento

Misure in essere e da adottare
(Regola 19.4)

Dopo aver esaminato nel paragrafo precedente i rischi che possono derivare ai dati sia da comportamenti degli operatori che da eventi relativi agli strumenti e al contesto si rende necessario dettagliare le misure di sicurezza in essere e da adottare a contrasto dei citati rischi. La misura in questo caso non deve essere intesa solo quale lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia ma deve essere considerata anche quell'insieme di attività di verifiche e controllo nel tempo, essenziali per assicurarne l'efficacia.
Infatti senza procedure di controllo periodico nessuna misura può essere considerata completa.
Per meglio individuare le misure in essere e quelle da adottare si fa riferimento alla tabella sotto riportata.

Tabella 4.1 misure di sicurezza adottate o da adottare

Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Misura già in essere	Misura da adottare	Data entro cui adottare la misura	Periodicità	Responsabile dei controlli
Formazione del personale	Il furto o lo smarrimento di credenziali e di autenticazione, la carenza di consapevolezza e incuria, il comportamento sleale o fraudolento, l'errore materiale, l'accesso non autorizzato ai locali da parte dei soggetti esterni, l'asportazione e il furto di strumenti contenenti i dati, eventi distruttivi naturali o artificiali dolosi ecc., guasto ai sistemi complementari	Tutti	Tutte	In essere			Annuale o al momento dell'assunzione	Servizio Affari Generali, Servizi Demografici,
Effettuare giornalmente il salvataggio dei dati	La carenza di consapevolezza, disattenzione incuria, errore materiale, azione di virus informatici, azione di hacker, asportazione e furto di strumenti contenenti dati, eventi distruttivi naturali o artificiali, guasti ai sistemi complementari	Tutti	Tutte	In essere			Giornaliera	Responsabile CED
Installazione appositi software per impedire ai dipendenti l'utilizzo di programmi non autorizzati	Evitare comportamenti sleali di dipendenti che installando software non autorizzati possano arrecare danni alle banche dati	Tutti	Tutte	In essere parzialmente in quanto in alcuni fattispecie queste			Aggiornamento dei software sulla base delle esigenze ...	Responsabile CED

				restrizioni non sono applicabili				
Attribuire la custodia dei software e delle relative licenze al responsabile CED	Evitare che i software vengano utilizzati da dipendenti per fini personali	Nessuna	Nessuna	In essere			Una tantum	Sindaco
Installazione e aggiornamenti programmi antivirus	Evitare l'intrusione di virus nel sistema	Tutti	Tutte	In essere			Aggiornamento almeno settimanale, il più delle volte quotidiano	Responsabile CED
Informazione ai dipendenti del divieto di installare programmi non autorizzati suscettibili di recare danni alle banche dati dell'ente	Rendere noto il contenuto del manuale operativo per la sicurezza	Tutti	Tutte	In essere	Emanare apposita circolare ed adottare il manuale sulle misure minime di sicurezza		Una Tantum e al momento dell'assunzione	Responsabile CED, Responsabile Personale
Installazione e aggiornamenti programmi antispamming	Evitare la saturazione inutile delle caselle e-mail con il rischio di importare virus	Tutti	Tutte	In essere			Aggiornamento almeno settimanale, il più delle volte quotidiano	Responsabile CED
~~Installazione e aggiornamenti programmi antispoofing~~	~~Evitare che gli hacker con appositi software siano in grado di utilizzare il vostro indirizzo e-mail~~	~~Tutti~~	~~Tutte~~	~~In essere~~			~~Aggiornamento Mensile~~	~~Responsabile CED~~
~~Installazione e aggiornamento programmi che evitino il tampering~~	~~Evitare che gli hacker con appositi software siano in grado di modificare il dato durante le transazioni~~	~~Tutti~~	~~Tutte~~	~~In essere~~			~~Aggiornamento Trimestrale~~	~~Responsabile CED~~
Disabilitare la risposta al ping sul firewall	Evitare che la linea ADSL sia satura e resa inutilizzabile dagli hacker	Nessuna	Nessuna	In essere			Una Tantum	Responsabile CED
Stipulare contratti di manutenzione dell'hardware e del software	Assicurare il perfetto funzionamento di tutto il sistema informatico al fine di prevenire la perdita di dati	Tutti	Tutte	In essere			Annuale	Responsabile CED
Prevedere la sostituzione dell'hardware all'occorrenza con	La sostituzione dell'hardware permette di avere un sistema informatico sempre	Tutti	Tutte	In essere	Dotarsi di appositi contratti che prevedano una celere sostituzione degli		All'occorrenza sentito il Responsabile CED	Responsabile CED

estrema sollecitudine	all'avanguardia ed in grado di assicurare il migliore trattamento dei dati possibile				strumenti qualora si renda necessario			
Evitare l'accesso ai locali da parte di personale non autorizzato	Evitare la diffusione di dati	Tutti	Tutte	Da adottare	Formare il personale al fine di renderlo edotto dei possibili rischi derivanti	31/12/2009	Una tantum o al momento dell'assunzione	Ogni dipendente
Dotare le apparecchiature informatiche di idonei sistemi di sicurezza (password) nonché per i pc portatili oltre a tali strumenti munirli di cavetto di sicurezza ed evitare di lasciarli incustoditi	Evitare che in caso di furto degli strumenti informatici possano essere utilizzati i dati in essi contenuti	Tutti	Tutte	In essere	Dotare tutti i pc di password alfanumeriche (minimo 8 caratteri), acquistare cavetto di sicurezza per i portatili, informazione al personale dipendente		Aggiornamento password trimestrale, Cavetto di sicurezza: una tantum ed all'occorrenza, Circolare al personale: una tantum	Responsabile CED, Responsabile Personale
Accertare il funzionamento dei sistemi di allarme degli uffici	Evitare l'ingresso di estranei al di fuori degli orari consentiti	Tutti	Tutte	In essere (solo per i Servizi Demografici)	Dotare di sistema di allarme la sede dell'Ente		Verifica semestrale del regolare funzionamento	Servizio Lavori Pubblici
Adozione di una cassaforte ignifuga dove riporre i salvataggi quotidiani	Evitare che in caso di eventi distruttivi vengano persi completamente tutti i dati	Tutti	Tutte	In essere				Servizio Finanziario
Depositare copia dei backup in luogo esterno alla struttura (cassaforte di sicurezza servizio finanziario)	Evitare che in caso di danni alla struttura vengano persi definitivamente tutti i dati	Tutti	Tutte	Da adottare	Incaricare un soggetto che porti nella sede indicata la copia dei dati almeno una volta settimana	31/12/2010	Una Tantum	Responsabile CED
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]
Dotare l'ente di gruppi di continuità	Consentire che in caso di guasti alla rete elettrica o in caso di interruzione della	Tutti	Tutte	In essere			Trimestralmente verificare il funzionamento	Responsabile CED

	somministrazione dell'energia sia possibile effettuare almeno il salvataggio dei dati							
Climatizzare il locale server o acquistare e mettere in opera un armadio chiuso a chiave e munito di ventilatori	Evitare che ci sia un surriscaldamento delle macchine con conseguente malfunzionamento e possibile perdita di dati.	Tutti	Tutte	In essere	Acquistare climatizzatori in numero e potenza sufficiente al locale server		Verifica Semestrale del regolare funzionamento	Responsabile CED

Criteri e modalità di ripristino della disponibilità dei dati
(Regola 19.5)

Tutte le banche dati gestite dall'ente vengono salvate automaticamente con frequenza giornaliera.
Tale aggiornamento è curato dal responsabile CED ed il salvataggio avviene mediante appositi dispositivi. Sull'etichetta del supporto contenente la copia dei dati viene riportata l'indicazione del giorno della settimana oltre al codice della stessa. Le procedure di back up devono essere eseguite in un momento di non attività degli incaricati ovvero questi devono essere preventivamente avvertiti di interrompere l'attività di trattamento.

La verifica del backup è effettuata confrontando le dimensioni dei file di backup con le dimensioni dei files originali; a discrezione del responsabile di backup potranno essere ripristinate delle copie in un elaboratore esplicitamente predisposto alla verifica del back up.

Il ripristino della banca dati è effettuato con modalità inverse a quelle di backup; la banca dati da ripristinare verrà copiata in una cartella temporanea e protetta da permessi d'accesso a cura del responsabile CED. La banca dati verrà spostata nella sede di quella danneggiata che verrà soprascritta o preventivamente distrutta.

~~Le prove di ripristino di efficacia delle procedure di salvataggio / ripristino dei dati adottate vengono effettuate ogni 3 mesi a cura del responsabile CED.~~

Pianificazione degli interventi formativi previsti
(Regola 19.6)

Nell'ambito della normativa in materia di protezione dei dati personali un ruolo importante e altrettanto delicato è quello della formazione del personale. Sarebbe infatti completamente inutile pensare solo ed esclusivamente all'attuazione della norma da parte di un gruppo ristretto di persone all'interno dell'ente senza sensibilizzare poi tutti i dipendenti in merito alle problematiche, ai rischi e alle responsabilità anche penali a cui tutti gli stessi sono soggetti.
Come in ogni nuova attività che viene posta in essere occorre porre una particolare attenzione, anche nell'ambito della privacy è necessario svolgere una formazione il più possibile capillare che raggiunga tutti i dipendenti indipendentemente dalla categoria giuridica di appartenenza; infatti nell'ambito della attività all'interno degli uffici qualsiasi dipendente ha la possibilità di venire a contatto con una serie di dati sottoposti alla normativa in materia di tutela dei dati personali. La formazione ha come obiettivo principale quello di sensibilizzare e rendere edotto il personale delle attività che devono essere attuate sia da un punto di vista normativo che da un punto di vista tecnico.
Il trattamento dei dati viene infatti svolto normalmente sia con strumenti elettronici che cartacei; in questa sede è opportuno andare ad esaminare i possibili rischi derivanti dall'utilizzo dei sistemi informatici.
Assicurare la miglior sicurezza dei Sistemi Informativi Automatizzati presenta particolari problematiche d'ordine culturale, sociale ed organizzativo oltre che legale e tecnico, per questo è anche necessario elaborare ed attuare specifici processi di formazione, sensibilizzazione e corresponsabilizzazione.
La sensibilizzazione alle tematiche della sicurezza informatica ed a costanti comportamenti coerenti con le politiche e le disposizioni date in merito, deve interessare tutte le risorse umane dell'Amministrazione, anche quelle non direttamente interessate dalla formazione predetta, ad ogni livello di responsabilità ed attività.
Ciò al fine di diffondere una cultura generalizzata della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese oltre che di sopperire ad eventuali mancanze delle stesse.

Per la corresponsabilizzazione, si deve prevedere di:

- Coinvolgere i Responsabili di servizio e rappresentanze degli addetti in tutte le fasi di definizione del piano per la sicurezza (analisi e gestione dei rischi, politiche, piano operativo e audit);
- Effettuare interventi di richiamo e se necessario adottare gli adeguati provvedimenti disciplinari in caso di inadempienze e/o superficialità in tema di sicurezza informatica.

Analoghi processi devono essere previsti con eventuali partner e per i collaboratori esterni, privati e pubblici, persone fisiche e giuridiche, che interagiscono in modo significativo con l'Amministrazione.
Infine, occorre informare e sensibilizzare su queste tematiche anche gli utenti finali dei servizi erogati dall'Amministrazione.
L'introduzione di un sistema di sicurezza, come di qualunque altro elemento che modifichi le modalità lavorative all'interno di una qualsiasi realtà, ha sicuramente un forte impatto sull'organizzazione.

La formazione interviene in due momenti ben precisi del processo di introduzione di un sistema di sicurezza:

- Sensibilizzazione sulle problematiche della sicurezza e sulla loro importanza
- Conoscenza delle misure di sicurezza da adottare e da gestire ai diversi livelli di responsabilità

Dunque anche i fruitori della formazione saranno di diversa tipologia: è fondamentale riuscire a sensibilizzare i Responsabili delle Amministrazioni affinché questi riescano a trasmettere i principi fondamentali del sistema all'interno delle loro realtà.
Per raggiungere i suoi obiettivi il programma di formazione deve essere concepito in modo tale da:

- Rendere consapevoli i partecipanti sull'importanza delle scelte aziendali;
- Coinvolgere i partecipanti sulle problematiche inerenti la sicurezza;
- Responsabilizzare i partecipanti sulle attività da eseguire per garantire il mantenimento di un livello di sicurezza accettabile.

Occorre quindi progettare un corso dove sono previsti cenni sulla normativa, indicazioni sulle Politiche di Sicurezza, analisi dei rischi, indicazioni precise sui comportamenti da adottare sia nelle operazioni quotidiane che nelle situazioni di emergenza.

Il corso sarà progettato in base alle diverse esigenze ed ai diversi sistemi di sicurezza sviluppati all'interno dell'ente, in funzione del patrimonio informativo da proteggere e dal grado di informatizzazione raggiunto; in generale non potranno mancare riferimenti a:

- Normativa vigente
- Definizione delle responsabilità
- Elenco delle vulnerabilità: spesso non c'è la consapevolezza dei rischi che si possono correre, vale quindi la pena individuare i punti di vulnerabilità del sistema, sia nell'ottica della prevenzione che nell'individuazione di possibili incidenti.
- Regole comportamentali che comprendono:
- Gestione degli accessi (password,...)
- I possibili rischi: virus, intercettazioni, intrusioni, ...
- Firma digitale.

L'Amministrazione deve tener presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a garantire il personale dal rischio di perdere o comunque compromettere parte del lavoro fatto.
La progettazione degli interventi formativi dovrà comunque rientrare tra le previsioni del piano annuale della formazione redatto in base alle norme vigenti.
Per il corrente anno si può ipotizzare l'intervento formativo riportato nella seguente tabella:

Tabella 6.1 Interventi formativi previsti

Corso di formazione	Descrizione sintetica	Classi di incarico interessati	Numero di incaricati interessati	Numero di incaricati già formati/ da formare nell'anno	Calendario
Il codice in materia di protezione dei dati personali: esame normativa, DPS e adempimenti conseguenti, analisi del manuale operativo, norme di comportamento per il trattamento e la tutela dei dati personali	Il corso ha quale obbiettivo quello di fornire a tutti i dipendenti le principali nozioni in merito alla normativa, ai principali adempimenti nonché all'esame del dps evidenziando le figure necessarie a dare attuazione a quanto previsto dalla normativa nonché le relative responsabilità, illustrare il manuale operativo sulla sicurezza nonché i comportamenti e gli accorgimenti da tenere	Tutti i dipendenti	Tutti	Tutti devono essere formati	31/12/2009

	per la salvaguardia dei dati				

Trattamenti affidati all'esterno
(Regola 19.7)

Nello svolgimento delle attività istituzionali l'ente si avvale della collaborazione di soggetti esterni che attuano comunque trattamento dei dati.
Dall'esame della situazione dell'ente emergono le attività affidate all'esterno riportate nella seguente tabella.

Tabella 7.1 Attività esternalizzate

Attività esternalizzata	**Descrizione sintetica**	**Dati personali, sensibili o giudiziari interessati**	**Soggetto esterno**
Servizio di tesoreria comunale	Viene gestito il servizio di cassa in entrata e uscita (es. Riversali, liquidazioni mandati, ecc..).	Non vengono trattati dati sensibili	Banca di Credito Cooperativo di Carugate
Riordino archivi	Interviene direttamente sugli archivi procedendo al loro riordino	Può venire a conoscenza di tutte le tipologie di dati	Bernini Daniela
Fornitura ed assistenza hardware	Fornitura ed assistenza hardware	Possono venire a conoscenza di tutte le tipologie di dati	Bit@Bit
Riscossione ruoli TARSU	Riscossione ruoli TARSU	Non vengono trattati dati sensibili	CEM S.p.A.
Fornitura software e manutenzione banche dati tributi e contabilità, anagrafe, stato civile, elettorale	Fornitura software e manutenzione banche dati tributi e contabilità, anagrafe, stato civile, elettorale	Possono venire a conoscenza di dati sensibili	Halley Informatica
Assistenza domiciliare minori e servizio psicologico	Assistenza domiciliare minori e servizio psicologico	Vengono trattati dati sensibili, giudiziari e personali	Bathor - Vigevano
SAD Anziani e disabili	SAD Anziani e disabili	Vengono trattati dati sensibili e sanitari	Consorzio Farsi Prossimo - Milano
Tributi Vari	Tributi Vari	Non vengono trattati dati sensibili	Esatri S.p.A.
Fornitura ed assistenza software	Fornitura ed assistenza software	Possono venire a conoscenza di tutte le tipologie di dati	Halley Informatica di Ciccolini G. & C. snc - Matelica
Redazione DPS	Redazione del Documento Programmatico per la Sicurezza dei dati	Possono venire a conoscenza di tutte le tipologie di dati	Halley Lombardia di Monti, Molteni & C. snc – Cantù
Gestione servizio acquedotto	Gestione servizio acquedotto	Potrebbe venire a conoscenza di dati sensibili	IDRA SPA
Gestione multe, cessioni di fabbricato e ospitalità stranieri	Gestione multe, cessioni di fabbricato e ospitalità stranieri	Potrebbero venire a conoscenza di dati sensibili	Maggioli SPA
Gestione impianti sportivi	Gestione impianti sportivi	Possono venire a conoscenza di dati sensibili e sanitari	Polisportiva Gessate
Revisore dei conti	Revisori dei conti	Possono venire a conoscenza di dati sensibili	Dr. Massimo Giudici
Gestione micronido	Gestione micronido	Vengono a conoscenza di dati sensibili	Scuola Materna STEFANO LATTUADA
Prestiti bibliotecari	Prestiti bibliotecari	Possono venire a conoscenza di dati sensibili	Sistema bibliotecario comunale – Melzo
Gestione servizi amministrativi refezione	Gestione servizi amministrativi refezione	Vengono trattati dati sensibili	Sodexo Italia S.p.A.

Gestione stipendi	Gestione stipendi	Possono venire a conoscenza di dati sensibili	Studio GARZON
Medico del lavoro	Medico del lavoro	Viene a conoscenza di dati sanitari	Studio R.L. SRL
Accertamenti ICI, bollettazione e rendicontazione ICI	Accertamenti ICI, bollettazione e rendicontazione ICI	Non vengono trattati dati sensibili	Tecnologia & Territorio
Gestione servizio gas	Gestione servizio gas	Potrebbe venire a conoscenza di dati sensibili	E On Rete Orobica s.r.l.
Servizi sociali vari	Vari	Vengono trattati dati sensibili, giudiziari e personali	Ufficio di Piano – Cernusco sul Naviglio
Trasporto documenti Enti Pubblici Milano	Trasporto documenti Enti Pubblici Milano	Potrebbero venire a conoscenza di dati sensibili	Zovi Paola

I soggetti esterni a cui viene affidato il trattamento devono assumersi già nei contratti degli impegni e precisamente il soggetto deve dichiarare:

- di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali
- di ottemperare agli obblighi previsti dal codice per la protezione dei dati personali
- di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere
- di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze
- di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate