COMUNE DI SAN VINCENZO VALLE ROVETO
Via Marconi, 7 – 67050
C. F. : 00217860667

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, LETTERA G) DEL D. LGS. 196/2003, E DEL DISCIPLINARE TECNICO ALLEGATO AL MEDESIMO DECRETO SUB B)

Il presente documento è redatto e firmato in calce dal Rappresentante Legale del **Comune di San Vincenzo Valle Roveto** Titolare del trattamento dei dati:

SINDACO
Dott. Carlo Rossi

2010

Conformemente a quanto prescrive il punto 19. del Disciplinare tecnico, allegato sub b) al D. lgs. 196/2003, nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare), mediante:
   - l'individuazione dei tipi di dati personali trattati;
   - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
   - l'elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti;
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati (analisi del mansionario privacy, punto 19.2 del disciplinare) e previsione di interventi formativi degli incaricati del trattamento (punto 19.6 del disciplinare);
3. l'analisi dei rischi che incombono sui dati (punto 19.3 del disciplinare);
4. le misure già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati (punto 19.4 del disciplinare);
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento (punto 19.5 del disciplinare);
6. i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno (punto 19.7 del disciplinare);
7. le procedure da seguire per il controllo sullo stato della sicurezza;
8. le dichiarazioni d'impegno e firma.

INDICE

L'ELENCO DEI TRATTAMENTI DEI DATI PERSONALI

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, si procede come segue:

- si individuano le tipologie di dati personali trattati, in base alla loro natura (sensibili, giudiziari e comuni) e le finalità che ne giustificano il trattamento;
- si descrivono le aree, i locali e gli strumenti con i quali si effettuano i trattamenti;
- si elabora la mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti.

Tipologie di dati trattati

I dati trattati dal Titolare si possono suddividere come segue:

1) Dati Sensibili idonei a rivelare lo stato di salute

- **Finalità**
  - Gestione del Personale
  - Gestione Protocollazione dei Documenti
  - Gestione dell'Ufficio Leva
  - Gestione dei Servizi Sociali
  - Gestione degli atti amministrativi e giudiziari di Polizia Municipale
  - Gestione delle assegnazioni di Case popolari
  - Gestione dell'Ufficio Segreteria e Affari Generali
  - Accertamenti sanitari per la scurezza nell'ambiente di lavoro
  - Gestione dell'Ufficio Commercio

2) Dati sensibili idonei a rivelare l'origine razziale od etnica

- **Finalità**
  - Gestione Protocollazione dei Documenti
  - Gestione dell'Ufficio Anagrafe
  - Gestione degli atti amministrativi e giudiziari di Polizia Municipale
  - Gestione delle assegnazioni di Case popolari
  - Gestione del Personale
  - Gestione dell'Ufficio Commercio

3) Dati sensibili idonei a rivelare le opinioni politiche, religiose, adesioni a partiti e sindacati;

- **Finalità**
  - Gestione Protocollazione dei Documenti
  - Gestione dell'Ufficio Elettorale
  - Gestione Economica del personale

4) Dati Giudiziari

- **Finalità**
  - Gestione Protocollazione dei Documenti
  - Gestione dell'Ufficio Elettorale
  - Gestione dell'Ufficio Leva
  - Gestione del Personale
  - Gestione dell'Ufficio Contenziosi Tributari
  - Gestione gare d'appalto dell'Ufficio Tecnico
  - Gestione dell'attività relativa alla repressione dell'abusivismo edilizio
  - Gestione del Deposito di Atti giudiziari
  - Gestione dei Servizi Sociali
  - Gestione degli atti amministrativi e giudiziari di Polizia Municipale
  - Gestione dell'Ufficio Segreteria e Affari Generali
  - Gestione dell'Ufficio Commercio

5) Dati Comuni (Identificativi)

- **Finalità**
  - Svolgimento, gestione ed organizzazione delle attività di tutte le Aree/Uffici dell'Ente.

Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

Il trattamento dei dati personali avviene nella sede principale situata in Via Marconi, 7 - CAP 67050, San Vincenzo Valle Roveto.
All'interno di tale sede vi sono i seguenti uffici dove avviene il trattamento dei dati:

NOME UFFICIO	ACCESSO			SISTEMA DI ALLARME	CHIUSURA CON SERRATURA	IMPIANTO CONDIZION.TO	FINESTRE CON GRATE
	PUBBLICO	CONTROLL.	REGISTRO				
Segreteria	No	Si	No	No	Si	No	No
Sindaco	No	Si	No	No	Si	No	No
Sala Riunioni	Si	No	No	No	Si	No	No
Protocollo	Si	Si	No	No	Si	No	No
Archivio Ragioneria	No	Si	No	No	Si	No	Non ci sono finestre
Amministrativo Tributi Elettorale	Si	Si	No	No	Si	No	Si
Corridoio	No	Si	No	No	Si	No	Non ci sono finestre
Ragioneria/ Tributi	Si	Si	No	No	Si	No	No
Tecnico	Si	Si	No	No	Si	No	No
Archivio Ufficio Tecnico	No	Si	No	No	Si	No	Non ci sono finestre
Archivio Ufficio operai	No	No	No	No	Si	No	Si
Vigilanza	Si	Si	No	No	Si	No	No
Anagrafe e Stato Civile	Si	Si	No	No	Si	No	Si
Archivio Anagrafe	No	Si	No	No	Si	No	Non ci sono finestre
Archivio Storico	No	Si	No	No	Si	No	Si

Strumenti mediante i quali viene effettuato Il trattamento dei dati

a) Schedari ed altri supporti cartacei

ARCHIVIO	TIPOLOGIA DATI TRATTATI	LOCALIZZAZIONE	DESCRIZIONE DEL TRATTAMENTO	ACCESSI
Delibere	Comuni.	Segreteria	Gestione e conservazione di delibere di Consiglio e di Giunta Comunale.	Musilli; Santomaggio; Scatena; Carnevale; Bisegna, Segretario.
Delibere	Comuni.	Archivio – Sala Riunioni	Gestione e conservazione di delibere di Consiglio e di Giunta Comunale	Tutti i dipendenti e gli amministratori.
Incarichi legali e Contratti	Comuni; Sensibili; Giudiziari.	Segreteria	Trattamento dati relativi a: conferimento di incarichi legali; Fascicoli cause e liti; stipulazione e registrazione dei contratti rogati dal segretario, delle convenzioni e degli altri contratti (compravendite, locazioni e concessioni).	Musilli; Santomaggio; Scatena; Carnevale; Bisegna.
Corrispondenza Ordinaria	Comuni; Sensibili; Giudiziari.	Sindaco	Trattamento dati relativi alla gestione della corrispondenza di competenza del sindaco.	Sindaco.
Elettorale (storico)	Comuni; Giudiziari.	Archivio – Sala Riunioni	Archiviazione fascicoli Elettorale anni pregressi	Tutti i dipendenti e gli amministratori.
Fascicoli Gare d'appalto	Comuni; Giudiziari.	Archivio – Sala Riunioni	Archiviazione Fascicoli Gare d'appalto.	Tutti i dipendenti e gli amministratori.
Protocollo	Comuni; Sensibili; Giudiziari.	Protocollo	Protocollazione, in entrata e in uscita, di tutti i documenti diretti all'ente e da questo prodotti e valutazione del contenuto degli stessi per assegnazione ai competenti uffici.	Tutto il personale
Protocollo	Comuni; Sensibili; Giudiziari.	Corridoio	Archiviazione fascicoli protocollazione anni pregressi.	Tutto il personale
Protocollo	Comuni; Sensibili; Giudiziari.	Archivio - Ufficio operai	Archiviazione fascicoli protocollazione anni pregressi	Tutto il personale
Mandati e Reversali	Comuni.	Archivio Ragioneria	Trattamento dati relativi a: Gestione ed archiviazione di mandati di pagamento, e reversali di incasso.	Tutto il personale

ARCHIVIO	TIPOLOGIA DATI TRATTATI	LOCALIZZAZIONE	DESCRIZIONE DEL TRATTAMENTO	ACCESSI
Originali di Mandati e Reversali	Comuni.	Corridoio	Archiviazione dei fascicoli originali di mandati di pagamento, reversali di incasso.	Tutto il personale
Mandati e Riversali - Fatture	Comuni.	Ragioneria/Tributi	Trattamento dati relativi a: Gestione ed archiviazione di mandati di pagamento, reversali di incasso, rendiconti e fatture.	Santomaggio
Determine	Comuni.	Amministrativo - Tributi - Elettorale	Raccolta determinazioni di area.	Musilli
Tributi	Comuni.	Amministrativo - Tributi - Elettorale	Trattamento dei dati relativi alla gestione dei contribuenti TARSU, TOSAP; Utenti del servizio Idrico; Interscambio informazioni con Uffici Comunali ed altri Enti ed Autorità.	Musilli
Tributi	Comuni.	Ragioneria -Tributi	Trattamento dei dati relativi alla gestione dei contribuenti ICI; Ricevute versamenti TARSU. Utenti del servizio Idrico; Trattamento dati relativi a contenziosi tributari.	Santomaggio
Elettorale	Comuni; Sensibili (Origine razziale ed etniche; Stato di salute; opinioni politiche); Giudiziari.	Amministrativo - Tributi - Elettorale	Trattamento dati per attività di: Gestione delle liste elettorali e delle consultazioni elettorali; Archiviazione schede e fascicoli dei cittadini votanti residenti e residenti all'estero.	Musilli
Sociale	Comuni; Sensibili (Origine razziale ed etniche; Stato di salute); Giudiziari.	Amministrativo - Tributi - Elettorale	Trattamento dati relativi alla gestione del servizio Sociale.	Musilli
Sociale	Comuni; Sensibili (Origine razziale ed etniche; Stato di salute); Giudiziari.	Corridoio	Archiviazione dei fascicoli inerenti il settore sociale.	Tutto il personale
Scuola	Comuni; Sensibili (Stato di salute).	Amministrativo - Tributi - Elettorale	Raccolta nominativi iscritti scuole pubbliche, utenti dei servizi mensa e scuolabus.	Musilli

ARCHIVIO	TIPOLOGIA DATI TRATTATI	LOCALIZZAZIONE	DESCRIZIONE DEL TRATTAMENTO	ACCESSI
Concessioni Cimiteriali	Comuni.	Amministrativo - Tributi - Elettorale	Trattamento dati relativi alla gestione delle concessioni cimiteriali.	Musilli
Gare e contratti area amministrativa	Comuni; Giudiziari.	Amministrativo - Tributi - Elettorale	Trattamento dati relativi alla gestione delle gare e contratti di area.	Musilli
Cartellini presenze dei dipendenti	Comuni.	Amministrativo - Tributi - Elettorale	Trattamento dati relativi alla gestione delle presenze ed assenze dei dipendenti.	Musilli
Gestione del Personale	Comuni; Sensibili (Origine razziale ed etniche; Stato di salute; Adesioni a partiti e sindacati; Convinzioni religiose); Giudiziari.	Ragioneria - Tributi	Trattamento dati riguardanti: le certificazioni di malattia, le ferie ed altri giustificativi delle assenze; prestazioni e compensi fuori dell'ente, pensionamenti e assegni familiari; Gestione del personale sotto il profilo economico, fiscale e previdenziale.	Santomaggio
Case Popolari	Comuni; Sensibili (Origine razziale ed etniche; Stato di salute).	Ragioneria/Tributi	Trattamento dati relativi alle utenze dei canoni di locazioni Case Popolari .	Santomaggio
Contratti ed elenco fornitori, creditori e debitori	Comuni	Ragioneria/Tributi	Trattamento dati relativi alla gestione dei contratti di locazione e dell'archivio fornitori, creditori e debitori.	Santomaggio
Determine	Comuni	Ragioneria - Tributi	Raccolta determinazioni Di Aree: Ragioneria; Tecnica e Amministrativa.	Santomaggio
Concessioni Edilizie	Comuni	Corridoio	Archiviazione dei fascicoli inerenti le concessioni edilizie.	Tutto il personale
Archivio Lavori Pubblici, Urbanistica e Edilizia Privata	Comuni; Sensibili (Origine razziali ed etniche, Stato di Salute); Giudiziari.	Archivio -Ufficio Tecnico	Archiviazione dei fascicoli inerenti tutta la documentazione di Lavori Pubblici, Urbanistica e Edilizia Privata.	Scatena; Carnevale.
Fascicoli Legge 81/08	Comuni; Sensibili (Stato di Salute).	Tecnico	Trattamento dati relativi agli Accertamenti sanitari per la scurezza nell'ambiente di lavoro (D. Lgs. 81/08).	Scatena; Carnevale.

ARCHIVIO	TIPOLOGIA DATI TRATTATI	LOCALIZZAZIONE	DESCRIZIONE DEL TRATTAMENTO	ACCESSI
Lavori Pubblici	Comuni; Sensibili (Origine razziali ed etniche; Stato di Salute); Giudiziari	Tecnico	Trattamento di tutti i dati relativi alla Gestione del Patrimonio: Gestione ed archiviazione dati relativi alle procedure di esproprio; Gestione beni demaniali (acquisizione, alienazioni, trasferimenti di diritti reali e gestione degli immobili, gestione inventari, gestione canoni di locazione e riscatto, morosità, recuperi e bollettazione) e manutenzione degli stessi; Gestione ed archiviazione dati relativi allo svolgimento di gare di appalto e progettazione di opere pubbliche. Archiviazione dati anagrafici di imprese; Archiviazione dati anagrafici di liberi professionisti; Comunicazioni all'autorità di Vigilanza; Adempimenti tecnici ed amministrativi relativi alle assegnazioni delle Case popolari.	Scatena; Carnevale.
Urbanistica e Edilizia Privata	Comuni; Giudiziari	Tecnico	Trattamento dati finalizzati allo Studio e alla Programmazione Urbanistica e Interventi Integrati sul Territorio. Trattamento dati relativi a titolari di concessioni e autorizzazioni edilizie, permessi di costruire, denunce di inizio attività, controllo e vigilanza sull'attività edilizia; Trattamento dati finalizzato a: Gestione ed archiviazione in tema di condoni edilizi; Svolgimento dell'attività relativa alla repressione dell'abusivismo edilizio; Rilascio attestati e certificati afferenti gli immobili e le loro pertinenze.	Scatena; Carnevale.
Anagrafe - Lampade Votive	Comuni	Archivio - Ufficio operai	Trattamento dati relativi agli utenti del servizio lampade votive.	Tutto il personale

ARCHIVIO	TIPOLOGIA DATI TRATTATI	LOCALIZZAZIONE	DESCRIZIONE DEL TRATTAMENTO	ACCESSI
Anagrafe - Casette Asismiche	Comuni	Archivio - Ufficio operai	Trattamento dati relativi all'anagrafe casette asismiche e ai relativi abitanti.	Tutto il personale
Polizia Amministrativa e Giudiziaria	Comuni; Sensibili (Origine razziali ed etniche; Stato di Salute); Giudiziari.	Vigilanza	Trattamento dati relativi a: Accertamenti anagrafici; Sequestri amministrativi; Accertamento Infortuni sul lavoro; Assunzioni lavoratori stranieri; Controlli e verifiche cittadini extracomunitari presenti sul territorio comunale; Comunicazioni cessione fabbricati; Permessi ed ordinanze. Trattamento dati per: attività di vigilanza edilizia relativa alla repressione dell'abusivismo e del danno ambientale; Attività di accertamento delle infrazioni amministrative e penali; esecuzione T.S.O. Attività di accertamento e acquisizione di notizie di reato, annotazioni all'A.G., sequestri amm.vi – giudiziari, accertamenti in materia di evasione dei tributi comunali; Attività di polizia mortuaria.	Cesarini
Polizia/Codice della strada	Comuni; Sensibili (Origine razziali ed etniche; Stato di Salute); Giudiziari	Vigilanza	Trattamento dati relativi a: Attività di Vigilanza in materia di polizia stradale; Accertamento, contestazione e gestione amministrativa delle infrazioni al Codice della Strada; Infortunistica stradale (rilievo e gestione amministrativa degli incidenti stradali); Rilascio contrassegno ai portatori di handicap.	Cesarini
Commercio e Attività produttive	Comuni; Sensibili (Origine razziali ed etniche; Stato di Salute); Giudiziari.	Vigilanza	Trattamento dati relativi a: Autorizzazioni e licenze per attività commerciali di somministrazione, commercio in sede fissa e su aree pubbliche; Libretti di idoneità sanitaria ed autorizzazioni sanitarie; Cessazioni attività commerciali	Cesarini

ARCHIVIO	TIPOLOGIA DATI TRATTATI	LOCALIZZAZIONE	DESCRIZIONE DEL TRATTAMENTO	ACCESSI
Anagrafe	Comune; Sensibile (Origine razziale ed etniche; Opinioni politiche, religiose, adesioni a partiti e sindacati; Stato di salute); Giudiziario.	Anagrafe-Stato Civile	Trattamento di tutti i dati contenuti negli archivi dell'anagrafe della popolazione residente e della popolazione residente all'estero (AIRE); Trattamento dati finalizzato all'espletamento delle pratiche relative alla presentazione delle istanze di rilascio e rinnovo dei permessi di soggiorno, delle carte di soggiorno e dei ricongiungimenti familiari Trattamento di dati per attività di: Gestione e rilascio certificazioni anagrafiche e carte d'identità. Censimento della popolazione; Elenchi dei Giudici popolari.	Musilli; Stallocca
Stato Civile	Comune; Sensibile (Origine razziale ed etniche; Stato di salute).	Anagrafe-Stato Civile	Trattamento dati per attività di: Gestione degli atti dei registri di Stato Civile e relativi aggiornamenti; Gestione e rilascio certificazioni di Stato Civile.	Musilli; Stallocca
Leva militare	Comune; Sensibile (Stato di salute).	Anagrafe-Stato Civile	Trattamento dati per attività di: Gestione e archiviazione delle liste di leva e dei ruoli matricolari.	Musilli; Stallocca
Archivio Anagrafe e Stato Civile	Comune; Sensibile (Origine razziale ed etniche; Opinioni politiche, religiose, adesioni a partiti e sindacati; Stato di salute); Giudiziario.	Anagrafe	Archiviazione fascicoli e documentazione Anagrafe e Stato Civile.	Musilli; Stallocca
Archivio Storico	Tutti	Archivio Storico	Archiviazione storica e classificazione della documentazione di tutte le Aree/Uffici dell'Ente.	Tutto il personale

b) Diritti di accesso alla Banche Dati Informatiche

NOME BANCA DATI		ACCESSI	DIRITTI DI ACCESSO				OUT-SOURCING
DESCRIZIONE	DATI		LETTURA/ STAMPA	INSERIM.	MODIF.	ANNULLA	
Banca dati Contabilità	**Comuni**						NO
		Santomaggio		**X**	**X**	**X**	NO
Banca dati Protocollo	**Comuni; Sensibili; Giudiziari**						
		Bisegna	**X**	**X**	**X**	**X**	NO
		Lancia	**X**	**X**	**X**	**X**	NO
				Solo in partenza			
		Musilli	**X**	**X**			NO
		Stallocca	**X**	**X**			NO
		Cesarini	**X**	**X**			NO
		Santomaggio	**X**	**X**			NO
		Scatena	**X**	**X**			NO
		Carnevale	**X**	**X**			NO
Banca dati Tributi	**Comuni**						
		Santomaggio		**X**	**X**	**X**	NO
		Musilli		**X**	**X**	**X**	NO
Banca dati Gestione Economica del Personale	**Comuni Sensibili**						
		Santomaggio		**X**	**X**	**X**	NO
Banca dati Dichiarazione dei Redditi/Modelli 770/CUD	**Comuni Sensibili**						
		Santomaggio		**X**	**X**	**X**	NO
Banca dati Concessioni Edilizie	**Comuni**						
		Scatena		**X**	**X**	**X**	NO
Banca dati Case Popolari	**Comuni Sensibili**						
		Scatena		**X**	**X**	**X**	NO
		Santomaggio		**X**	**X**	**X**	NO
		Bisegna		**X**	**X**	**X**	NO
		Farina	**X**				NO
Banca dati Anagrafe e Stato Civile	**Comuni; Sensibili; Giudiziari**						
		Musilli	**X**	**X**	**X**	**X**	NO
		Stallocca	**X**	**X**	**X**	**X**	NO

c) Elaboratori non in rete

Non presente

d) Elaboratori in rete privata con collegamento ad internet

UFFICIO	NOME PC	SISTEMA OPERATIVO
Segreteria	PC Segreteria Utilizzo: Claudio Rossi	Windows XP
Sindaco	PC Sindaco Utilizzo: Carlo Rossi	Windows 98
Protocollo	PC Protocollo Utilizzo: Bisegna e Lancia	Windows XP
Sala Riunioni	PC Server	Windows XP
Amministrativo Tributi Elettorale	PC Amministrativo Utilizzo: Musilli	Windows XP
Ragioneria	PC Ragioneria Utilizzo: Santomaggio	Windows XP
	PC Ragioneria Utilizzo: Bisegna	Windows XP
Tecnico	PC Tecnico 1 Utilizzo: Scatena	Windows XP
	PC Tecnico 2 Utilizzo: Carnevale	Windows XP
Archivio Ufficio operai	PC Archivio Utilizzo: Farina	Windows XP
Vigilanza	PC Vigilanza Utilizzo: Cesarini	Windows XP
Anagrafe Stato Civile	PC Anagrafe Utilizzo: Stallocca	Windows XP

e) Impianti di video sorveglianza

Non presenti.

f) Altri tipi di impianto

Non presenti.

La mappa dei trattamenti effettuati

Incrociando le coordinate di cui ai due paragrafi precedenti, si ottiene la mappa dei trattamenti di dati personali effettuati dal Titolare.

In relazione al diverso grado di rischio, è opportuno distinguere i trattamenti che sono posti in essere nelle tre distinte aree in cui sono dislocati gli strumenti, nei casi in cui la circostanza è significativa (per gli schedari e gli elaboratori non in rete).

Il simbolo X, apposto nella casella di incrocio, significa che determinati tipi di dati sono trattati con determinati strumenti:

BANCHE DATI E ARCHIVI CARTACEI	STRUMENTI UTILIZZATI					
	A	B	C	D	E	F
Banca dati Contabilità			X	X		
Banca dati Protocollo			X	X		
Banca dati Tributi			X	X		
Banca dati Gestione Economica del Personale			X	X		
Banca dati Dichiarazione dei Redditi/Modelli 770/CUD			X	X		
Banca dati Concessioni Edilizie			X	X		
Banca dati Case Popolari			X	X		
Banca dati Anagrafe e Stato Civile			X	X		
Files e Archivi informatici Tributi			X	X		
Files e Archivi informatici Elettorale			X	X		
Files Comunicazioni Amministrative			X	X		
Files Comunicazioni Segreteria			X	X		
Files Contrattualistica (Segreteria)			X	X		
Files di gestione quotidiana delle attività di Protocollo			X	X		
Files di gestione delle attività della Polizia Municipale			X	X		
Files di gestione delle attività inerenti il trattamento economico, fiscale e previdenziale del personale (Ragioneria).			X	X		
Files di gestione quotidiana delle attività Dell'Ufficio Tecnico - Lavori Pubblici			X	X		
Files di gestione quotidiana delle attività dell'Ufficio Tecnico - Urbanistica e edilizia privata			X	X		
Files di gestione Lampade Votive e Casette Asismiche			X	X		
Archivio Delibere	X					
Archivio Incarichi legali e Contratti	X					
Archivio Corrispondenza Ordinaria	X					
Archivio Elettorale (storico)	X					
Archivio Fascicoli Gare d'appalto	X					
Archivio Protocollo	X					
Archivio Originali di Mandati e Reversali	X					
Archivio Mandati e Riversali - Fatture	X					
Archivio Determine	X					
Archivio Tributi	X					
Archivio Elettorale	X					
Archivio Scuola	X					
Archivio Concessioni Cimiteriali	X					
Archivio Gare e contratti area amministrativa	X					
Archivio Cartellini presenze dei dipendenti	X					
Archivio Gestione del Personale	X					

BANCHE DATI E ARCHIVI CARTACEI	STRUMENTI UTILIZZATI					
	A	B	C	D	E	F
Archivio Case Popolari	X					
Archivio Contratti ed elenco fornitori, creditori e debitori	X					
Archivio Determine	X					
Archivio Lavori Pubblici	X					
Archivio Fascicoli Gare d'appalto	X					
Archivio Urbanistica e Edilizia Privata	X					
Archivio Concessioni Edilizie	X					
Archivio Lavori Pubblici, Urbanistica e Edilizia Privata	X					
Archivio Fascicoli Legge 626	X					
Anagrafe Lampade Votive	X					
Archivio Anagrafe Casette Asismiche	X					
Archivio Polizia Amministrativa e Giudiziaria	X					
Archivio Polizia/Codice della strada	X					
Archivio Commercio e attività produttive	X					
Archivio Anagrafe	X					
Archivio Stato Civile	X					
Archivio Leva militare	X					
Archivio Anagrafe e Stato Civile	X					

Legenda degli strumenti utilizzati per il trattamento dei dati e dei sistemi di sicurezza:

A. Schedari e altri supporti cartacei
B. Elaboratori non in rete
C. Elaboratori in rete privata
D. Elaboratori in rete pubblica
E. Impianti di video sorveglianza
F. Altri tipi di sistemi d'allarme e controllo

MANSIONARIO PRIVACY: RESPONSABILI ED INTERVENTI FORMATIVI DEGLI INCARICATI

Per il trattamento dei dati personali, il Titolare ha nominato i seguenti **RESPONSABILI**, attribuendo loro incarichi di ordine organizzativo e direttivo, come segue:

- Responsabile del trattamento dei dati personali inerenti lo svolgimento della Funzione di Segretario Comunale**: CLAUDIO ROSSI**
- Responsabile del trattamento dei dati personali Area Amministrativa **ORAZIO MUSILLI**
- Responsabile del trattamento dei dati personali Area Finanziaria **MALVINA SANTOMAGGIO**
- Responsabile del trattamento dei dati personali Area Tecnica **DOMENICO SCATENA**
- Responsabile del Back-up e della custodia delle copie di sicurezza delle banche dati **Massimiliano Bisegna**

Tutte le precedenti e le seguenti nomine sono state effettuate a mezzo di lettere di incarico, in cui sono specificate le responsabilità che sono state affidate a tutti i Responsabili, e sono state controfirmate dagli interessati per accettazione.

Ora andiamo ad elencare gli **INCARICATI DEL TRATTAMENTO** dei dati personale che a loro volta sono stati individuati dai vari RESPONSABILI delle singole Aree:

AREA AMMINISTRATIVA

- Incaricato del trattamento dei dati personali **MASSIMILIANO BISEGNA**
- Incaricato del trattamento dei dati personali **ANTONIO OSVALDO LANCIA**
- incaricato del trattamento dei dati personali **STALLOCCA LETIZIA**
- incaricato del trattamento dei dati personali **ELISABETTA CESARINI**

AREA TECNICA

- incaricato del trattamento dei dati personali **MAURO FARINA**
- incaricato del trattamento dei dati personali **CLAUDIO CARNEVALE**
- incaricato del trattamento dei dati personali **DUILIO BONADIES**

Soggetti incaricati

Il trattamento dei dati personali è effettuato solamente dai soggetti che hanno ricevuto un formale incarico, mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito. Le lettere di incarico che vanno a completare il mansionario sono allegate al presente documento. Allegato B.

Istruzioni specifiche fornite ai soggetti incaricati

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati sono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune;
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti;
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave;
- prescrizione per non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di custodia ed utilizzo dei supporti rimovibili, contenenti dati personali
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, è prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati sono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa nell'ambito del trattamento dei dati personali.
Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.
La stessa operazione è compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

Nel seguente elenco sono riassunti i tratti salienti dell'attuale mansionario privacy, come segue:

g) Il punto elenco principale riporta i dati personali oggetto di trattamento, quali emergono dall'analisi effettuata nel § 1, cap. 1 del presente documento;
h) Il punto elenco secondario riporta le unità organizzative in cui si suddivide l'organizzazione del Titolare;

i) Il fatto che un'unità organizzativa si trovi raggruppata su un determinato punto elenco, significa che una determinata unità organizzativa procede al trattamento dei dati indicati nel punto elenco.

1) Dati Sensibili idonei a rivelare lo stato di salute

- **Uffici**

  - Ufficio Sindaco
  - Ufficio Segreteria
  - Ufficio Protocollo
  - Corridoio
  - Archivio - Ufficio Operai
  - Ufficio Ragioneria e Tributi
  - Ufficio Amministrativo Tributi ed Elettorale
  - Ufficio Tecnico
  - Ufficio - Archivio Tecnico
  - Ufficio Vigilanza
  - Ufficio Anagrafe e Stato Civile
  - Archivio Anagrafe
  - Archivio Storico

2) Dati sensibili idonei a rivelare l'origine razziale ed etnica

- **Uffici**

  - Ufficio Sindaco
  - Ufficio Segreteria
  - Ufficio Protocollo
  - Corridoio
  - Archivio - Ufficio Operai
  - Ufficio Ragioneria e Tributi
  - Ufficio Amministrativo Tributi ed Elettorale
  - Ufficio Tecnico
  - Ufficio - Archivio Tecnico
  - Ufficio Vigilanza
  - Ufficio Anagrafe e Stato Civile
  - Archivio Anagrafe
  - Archivio Storico

3) Dati sensibili idonei a rivelare le opinioni politiche, religiose, adesioni a partiti e sindacati;

- **Uffici**

  - Ufficio Sindaco
  - Ufficio Protocollo
  - Ufficio Ragioneria e Tributi
  - Ufficio Tributi ed Elettorale

4) Dati Giudiziari

- **Uffici**

  - Ufficio Sindaco
  - Ufficio Segreteria
  - Ufficio Archivio - Sala Riunioni
  - Ufficio Protocollo
  - Corridoio
  - Archivio - Ufficio Operai
  - Ufficio Ragioneria e Tributi
  - Ufficio Amministrativo Tributi ed Elettorale
  - Ufficio Tecnico
  - Ufficio - Archivio Tecnico
  - Ufficio Vigilanza
  - Ufficio Anagrafe e Stato Civile
  - Archivio Anagrafe
  - Archivio Storico

5) **Dati Comuni (Identificativi)**
   - **Uffici**
     - Ufficio Sindaco
     - Ufficio Segreteria
     - Ufficio Archivio - Sala Riunioni-
     - Archivio - Ufficio Operai
     - Ufficio Protocollo
     - Corridoio
     - Ufficio Ragioneria e Tributi
     - Ufficio Amministrativo Tributi ed Elettorale
     - Ufficio Tecnico
     - Ufficio - Archivio Tecnico
     - Ufficio Vigilanza
     - Ufficio Anagrafe e Stato Civile
     - Archivio Anagrafe
     - Archivio Storico

Sono previsti ***interventi formativi degli incaricati del trattamento***, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per la sicurezza o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.
In ogni caso, è prevista una riunione annuale per fare il punto sull'evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali.

AMMINISTRATORI DI SISTEMA

Con la definizione di «amministratore di sistema» si individuano, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini della normativa sulla Privacy (***Provvedimento del Garante 27/11/08***) vengono pero' considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Gli amministratori di sistema cosi' ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attivita' sono, in molti casi, concretamente «responsabili» di specifiche fasi lavorative che possono comportare elevate criticita' rispetto alla protezione dei dati.
Attivita' tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacita' di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; cio', anche quando l'amministratore non consulti «in chiaro» le informazioni medesime. La rilevanza, la specificita' e la particolare criticita' del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualita' di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615-ter) e di frode informatica (art. 640-ter), nonche' per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (articoli 635-bis e ter) e di danneggiamento di sistemi informatici e telematici (articoli 635-quater e quinques) di recente modifica.
È chiara la necessita' di prestare massima attenzione ai rischi e alle criticita' implicite nell'affidamento degli incarichi di amministratore di sistema nonché di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualita' di amministratore di sistema; richiama inoltre l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Cio', tenendo in considerazione l'opportunita' o meno di tale attribuzione e le concrete modalita' sulla base delle quali si svolge l'incarico, unitamente alle qualita' tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilita', specie di ordine penale e civile (articoli 15 e 169 del Codice), che possono derivare in caso di incauta o inidonea designazione.
Di seguito sono indicati gli accorgimenti e le misure che vengono adottati ai sensi dell'art. 154, comma 1, lettera c) del Codice, esclusi quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che, ponendo minori rischi per gli interessati, sono stati oggetto delle recenti misure di semplificazione (art. 29 decreto-legge 25 giugno 2008, n. 112, convertito, con modifiche, con legge 6 agosto 2008, n. 133; art. 34 del Codice; provv. Garante 6 novembre 2008).

Valutazione delle caratteristiche soggettive. L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacita' e dell'affidabilita' del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

Designazioni individuali. La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operativita' consentiti in base al profilo di autorizzazione assegnato.

Elenco degli amministratori di sistema. Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento da mantenere aggiornato e disponibile in caso di accertamenti.

Verifica delle attivita'. L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attivita' di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Registrazione degli accessi. Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

Si stima il grado di rischio, che dipende dalla tipologia dei dati trattati dal Titolare, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

Tabella rischi software:

TIPO DI RISCHIO	SOFTWARE	DATI	GRADO DI RISCHIO
Perdita di dati dolose; Perdita di dati accidentale.	Microsoft Office	Comuni; Sensibili; Giudiziari.	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Anagrafe	Comuni; Sensibili; Giudiziari	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Contabilità	Comuni	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Protocollo	Comuni; Sensibili; Giudiziari	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Tributi	Comuni	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Gestione Economica del Personale	Comuni; Sensibili.	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Dichiarazione dei Redditi/Modelli 770/CUD	Comuni; Sensibili.	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Concessioni Edilizie	Comuni	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Case Popolari	Comuni; Sensibili.	Basso
Perdita di dati dolose; Perdita di dati accidentale.	Anagrafe e Stato Civile	Comuni; Sensibili.	Basso

Tabella rischi hardware:

TIPO DI RISCHIO	NOME PC E SISTEMA DI ELABORAZIONE	BANCA DATI E FILES SALVATI SUL PC	GRADO DI RISCHIO
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	Server / WINDOWS XP Home	Pacchetto Office	Basso
		Banca dati Anagrafe e Stato Civile	
		Banca dati Contabilità	
		Banca dati Protocollo	
		Banca dati Tributi	
		Banca dati Gestione Economica del Personale	
		Banca dati Dichiarazione dei Redditi/Modelli 770/CUD	
		Banca dati Concessioni Edilizie	
		Banca dati Case Popolari	
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Anagrafe/ Windows 2000 Professional	Banca dati Anagrafe e Stato Civile	Basso
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Tributi/ WINDOWS XP Home	Files e Archivi informatici Tributi	Basso
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Amministrazione/ Windows XP Home	Files e Archivi informatici Elettorale	Basso
		Files Comunicazioni Amministrative	
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Segreteria / Windows XP Home	Files Comunicazioni Segreteria	Basso
		Files Contrattualistica (Segreteria)	

TIPO DI RISCHIO	NOME PC E SISTEMA DI ELABORAZIONE	BANCA DATI E FILES SALVATI SUL PC	GRADO DI RISCHIO
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Protocollo Windows XP	Files di gestione quotidiana delle attività di Protocollo	Basso
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Vigilanza/ WINDOWS XP	Files di gestione quotidiana delle attività della Polizia Municipale	Basso
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Ragioneria/ Windows XP	Files di gestione quotidiana delle attività inerenti il trattamento economico, fiscale e previdenziale del personale (Ragioneria)	Basso
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Tecnico 2/ WINDOWS XP	Files di gestione quotidiana delle attività Dell'Ufficio Tecnico - Lavori Pubblici	Basso
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Tecnico 1/ Windows XP	Files di gestione quotidiana delle attività dell'Ufficio Tecnico -Urbanistica e edilizia privata	Basso
Perdita di dati per malfunzionamento unità di memoria. Perdita di dati per malfunzionamento unità a disco. Perdita di dati conseguente alla rottura dei dischi magnetici. Mancato accesso ai dati per difetto all'unità di alimentazione. Mancato accesso ai dati per difetto ad altre unità.	PC Archivio / WINDOWS XP	Files di gestione Utenze Lampade Votive e Casette Asismiche	Basso

Si nota che un grado di rischio alto, o addirittura elevatissimo, è collegato al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- quelli idonei a rivelare informazioni di carattere sensibile o giudiziario dei soggetti interessati, che sono accomunati dall'aspetto critico di avere un elevato grado di pericolosità per la privacy dei soggetti interessati;
- quelli che costituiscono una importante risorsa, commerciale e tecnologica, per il Titolare, in relazione ai danni che conseguirebbero da una eventuale perdita, o trafugamento, dei dati.

Per quanto concerne ***gli strumenti impiegati per il trattamento***, le componenti di rischio possono essere idealmente suddivise in:

1. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato
   sostanzialmente:
   - al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti);
   - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici).
2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti).
3. rischio di penetrazione logica nelle reti di comunicazione.
4. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti.

Procedendo l'analisi dei rischi si è tenuto conto anche di alcuni fattori legati alla struttura del Titolare, nei seguenti termini:

- il rischio d'area, (legato alla eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento) è minimo, in quanto i trattamenti avvengono all'interno di uffici ad accesso controllato, con conseguente diminuzione del rischio:
  - per gli archivi esistenti in tali uffici;
  - per gli elaboratori in rete privata, in relazione al fatto che i server sono ubicati in tali uffici;
  - per i personal computer non in rete, localizzati in tali uffici.

- il rischio di guasti tecnici delle apparecchiature interessa i soli strumenti elettronici: in tale contesto, è giudicata più rischiosa la situazione degli strumenti non in rete che, essendo affidati a singoli che non sempre possiedono un bagaglio tecnico adeguato, presentano un rischio di rottura maggiore, rispetto agli impianti che sono gestiti da persone con specifiche competenze, quali quelli in rete e quello di sorveglianza;
- il rischio di penetrazione logica nelle reti di comunicazione interessa, essenzialmente, i soli strumenti che sono tra loro collegati tramite una rete di comunicazione accessibile al pubblico;
- il rischio legato ad atti di sabotaggio, o ad errori umani delle persone, presente in tutte le tipologie di strumenti utilizzati, è maggiore per quelli che sono in rete.

MISURE ATTE A GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI

Nel presente paragrafo sono descritte le misure atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

Si procede alla descrizione:

- delle misure che risultano già adottate dal Titolare, nel momento in cui è redatto il presente documento;
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata, anche per adeguarsi alle novità introdotte dal D. lgs. 196/2003, e dal disciplinare tecnico in materia di misure minime di sicurezza, allegato a tale decreto sub b).

La protezione di aree e locali

Per quanto concerne i rischi relativi alle strutture (rischio di area e misure atte a impedire gli accessi non autorizzati) si specifica che i locali sono protetti nel seguenti modo:

UFFICIO	INDIRIZZO	CHIUSURA CON SERRATURA	IMPIANTI DI CONDIZIONAMENTO	FINESTRE CON GRATE
Segreteria	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	No
Sindaco	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	No
Archivio Sala Riunioni	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	No
Protocollo	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	No
Sala Server	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	Non ci sono finestre
Amministrativo Tributi Elettorale	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	Si
Corridoio	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	Non ci sono finestre
Ragioneria Tributi	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	No
Tecnico	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	No

UFFICIO	INDIRIZZO	CHIUSURA CON SERRATURA	IMPIANTI DI CONDIZIONAMENTO	FINESTRE CON GRATE
Archivio Ufficio Tecnico	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	Non ci sono finestre
Archivio Ufficio operai	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	Si
Vigilanza	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	No
Anagrafe Stato Civile	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	Si
Archivio Anagrafe	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	Non ci sono finestre
Archivio Storico	Via Marconi, n. 7 67050, San Vincenzo Valle Roveto	Si	No	Si

Gli impianti ed i sistemi di cui è dotata l'organizzazione appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per l'anno sono quindi previsti semplicemente interventi di manutenzione.

La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli incaricati sono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento, o direttamente al titolare.
Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che sono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.
Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale che ai dati non possano accedere persone prive di autorizzazione.

I locali sono dotati dei seguenti accorgimenti:

UFFICIO	TIPO DI ARMADI				SCAFFALATURE	TIPO CASSETTI		CASSAFORTE	FINESTRE CON GRATE
	BLINDATI	IGNIFUGHI	SENZA SERRATURA	CON SERRATURA		SENZA SERRATURA	CON SERRATURA		
Segreteria	No	Si	No	Si	No	No	No	No	No
Sindaco	No	Si	No	Si	Si	No	No	No	No
Archivio sala riunioni	No	Si	No	Si	No	No	No	No	No
Protocollo	No	No	No	Si	Si	No	No	No	No
Sala Server	No	Si	Non ci sono finestre	No	Si	No	No	No	No
Amministrativo - Tributi - Elettorale	No	No	No	No	Si	No	No	No	No
Corridoio	No	No	Non ci sono finestre	No	No	No	No	Si	No
Ragioneria - Tributi	No	No	No	No	Si	No	No	No	No
Tecnico	No	Si	No	No	No	No	No	No	No
Archivio - Ufficio Tecnico	No	Si	Non ci sono finestre	No	Si	No	No	No	No
Archivio - Ufficio operai	No	Si	Si	Si	No	No	No	Si	Si
Vigilanza	No	No	Si	No	No	No	No	No	No
Anagrafe - Stato Civile	No	No	Si	Si	No	No	No	No	Si
Archivio - Anagrafe	No	Si	Non ci sono finestre	No	Si	No	No	Si	Non ci sono finestre
Archivio Storico	No	Si	Si	No	No	No	No	No	No

Tali strutture sono preposte a conservare i documenti e vengono utilizzare per riporre gli stessi in condizioni di sicurezza quando coloro che li hanno utilizzati si assentano dal lavoro anche temporaneamente. In caso di presenza di collaboratori o dipendenti costoro sono informati della necessità di restituire all'archivio o riporre i documenti laddove siano conservati in condizioni di sicurezza e secondo le disposizioni del titolare al trattamento o dei suoi incaricati o responsabili se individuati.

Tali strutture sono preposte a conservare i documenti e vengono utilizzare per riporre gli stessi in condizioni di sicurezza quando coloro che li hanno utilizzati si assentano dal lavoro anche temporaneamente. In caso di presenza di collaboratori o dipendenti

costoro sono informati della necessità di restituire all'archivio o riporre i documenti laddove siano conservati in condizioni di sicurezza e secondo le disposizioni del titolare al trattamento o dei suoi incaricati o responsabili se individuati.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa deve avvenire in luoghi , armadi , casseforti, o dispositivi equipollenti, che possono essere chiusi.

Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione di opportuni accorgimenti

Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici, si adottano le seguenti misure:

- Realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato.
- Realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative.
- Realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono Virus o altro tipo di "Malware".
- Prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD, ecc.), nei quali siano contenuti dati personali.

Il sistema di autenticazione informatica è adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:
- non contengono dati personali;
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle *credenziali di autenticazione* per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si utilizza il seguenti metodo:

- si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato esse sono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.

Dal momento che una componente della credenziale di autenticazione è costituita dal codice per l'identificazione (username), attribuito all'incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi; è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento;
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Agli *incaricati sono impartite precise istruzion*i in merito ai seguenti punti:

- Dovere di custodire i dispositivi, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici (ad esempio, il tesserino magnetico o la smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici (è prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'incaricato provveda a portare il dispositivo con sé (è prescritto l'obbligo di custodirlo come se fosse una carta di credito).
  In ipotesi di smarrimento, l'incaricato deve provvedere immediatamente a segnalare la circostanza all'amministratore di sistema, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo.

- Obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza.
- Dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:

- immediatamente, non appena è consegnata loro da chi amministra il sistema;
- successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

Le password sono composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici);
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata,
- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo è loro indicato al momento dell'attribuzione della password.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Per quanto concerne le *tipologie di dati ai quali gli incaricati possono accedere*, ed i trattamenti che possono effettuare, si osserva che:
- si è impostato un sistema di autorizzazione, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative.

Queste autorizzazioni all'accesso sono state rilasciate e possono essere revocate dal responsabile.

Il profilo di autorizzazione non viene in genere studiato per ogni singolo incaricato, ma è generalmente impostato per classi omogenee di incaricati (ad esempio, attribuendo

un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale). L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato o di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.
Annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

Per quanto riguarda la *protezione, di strumenti e dati*, da malfunzionamenti, attacchi informatici e programmi che contengono Virus o altro tipo di "Malware", sono adottate le misure sotto descritte.
Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).
A tale fine, si è dotati di idonei strumenti elettronici e programmi, che il D.lgs. 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento, di regola:

RETE	TIPO DI ANTIVIRUS	FREQUENZA DI AGGIORNAMENTO	DESCRIZIONE	NOME PC
LAN	Symantec Norton Antivirus	Giornaliera	Antivirus client/server	Tutti i Pc dell'Ente

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati;
Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Per quanto concerne i *supporti rimovibili* (es. floppy disk, dischi ZIP, CD.), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.
La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:
- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono

essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Nel corso del periodo di validità del presente documento sono previsti interventi di rinnovo e miglioramento.

CRITERI E MODALITÀ DI RIPRISTINO DEI DATI

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, sono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.

Per i dati trattati con strumenti elettronici, sono previste procedure di back-up, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi opportuni.

Il salvataggio dei dati trattati avviene come segue:

NOME PC	TIPO DI DATI	RESPONSABILE DEL BACK-UP	PERIODICITÀ DEL BACK-UP	SUPPORTO	NUM. SUPPORTI UTILIZZATI	NUM. COPIE DI BACK-UP
PC Server	Comuni; Sensibili; Giudiziari.	Bisegna; Massimiliano.	Giornaliero	DAT	2	1

Le copie vengono custodite:

NOME PC	TIPO DI DATI	RESPONSABILE DELLA CUSTODIA	LUOGO DI CONSERVAZIONE	NUM COPIE
PC Server	Comuni; Sensibili; Giudiziari.	Bisegna; Massimiliano.	Ufficio Protocollo - Cassetto chiuso a chiave	1

L'AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal D. lgs. 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.
Per la generalità dei casi, in cui il trattamento di dati personali, ***di qualsiasi natura***, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal D. lgs. 196/2003, se il terzo destinatario è italiano;
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

Qualora il trasferimento avvenga verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 D.lgs. 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.
Nei casi in cui il trattamento affidato all'esterno abbia per oggetto **dati *sensibili o giudiziari***, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.
Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano:
- rilasci una dichiarazione di avere adottato all'interno della propria struttura tutte le misure minime di sicurezza dettate dalla normativa.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta (allegata a questo documento).

Allo stato attuale risultano nominati come **responsabili/incaricati in out-sourcing:**

SOGGETTO	ATTIVITA'	TIPOLOGIA DEI DATI
Gerit S.p.a.	Gestione del servizio di riscossione TARSU	Comuni
Tinn Service s.r.l	Manutenzione e assistenza software	Comuni, Sensibili, Giudiziari

CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA

Al responsabili per la sicurezza è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.
Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile del trattamento dei dati personali o le persone da questo appositamente incaricate provvedono, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento;
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici;
- verificare l'integrità dei dati e delle loro copie di back-up;
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

DICHIARAZIONI D'IMPEGNO E FIRMA

Il presente documento, redatto nel mese di Marzo 2010 , viene firmato in calce da:

Rappresentante legale del Comune di San Vincenzo Valle Roveto, Titolare del trattamento dei dati nella persona di: **Carlo Rossi**.

L'originale del presente documento è custodito presso la sede dell'Ente Locale, per essere esibito in caso di controlli.

Una sua copia sarà consegnata:
- a ciascun responsabile interno del trattamento dei dati personali;
- a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

Nella relazione accompagnatoria del bilancio di esercizio si riferisce dell'avvenuta redazione del presente documento, che costituisce la prima redazione del Documento.

San Vincenzo Valle Roveto, 16/03/2010

Firma del Responsabile Generale del trattamento dei dati personali

……..……