ALLEGATO 9
PIANO PER LA SICUREZZA INFORMATICA

Questa ente, con deliberazione della Giunta Comunale n. 63 in data 15.09.2016, ha adottato il DPS (Documento Programmatico sulla Sicurezza), ai sensi del decreto legislativo 30.06.2003, n. 196.

Comune di Saltrio

Provincia di VA

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

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

Allegato alla deliberazione n. 63 assunta dalla
Giunta Comunale nella seduta del 15.09.2016

IL SINDACO

ing. Maurizio ZANUSO

IL SEGRETARIO COMUNALE

dott. Giuseppe CARDILLO

INDICE

1. PREMESSA

2. ELENCO DEI TRATTAMENTI DEI DATI PERSONALI (Regola 19.1)

3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ (Regola 19.2)

4. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (Regola 19.3)

5. MISURE IN ESSERE E DA ADOTTARE (Regola 19.4)

6. CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI (Regola 19.5)

7. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI (Regola 19.6)

8. TRATTAMENTI AFFIDATI ALL'ESTERNO (Regola 19.7)

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. 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. 196/03 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:
- Amministratore di sistema: deliberazione del Consiglio Comunale n. 23 in data 12.07.2012, di approvazione della convenzione con la Comunità Montana del Piambello per la gestione della figura dell’amministratore di sistema per il periodo 01.01.2013 / 31.12.2015;
- Amministratore di sistema: deliberazione del Consiglio Comunale n. 31 in data 28.07.2015, di approvazione della convenzione con la Comunità Montana del Piambello per la gestione della figura dell’amministratore di sistema per il periodo 01.01.2016 / 31.12.2018;
- Privacy: studio di ingegneria dott. ing. Davide BRESSAN – Piazza Trento e Trieste n. 2 – Busto Arsizio (VA)

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		Assistenza Sociale	Affari Generali	Server, Personal computer e archivi cartacei
2	Dati idonei a rivelare lo stato di disabilità	SI		Assistenza Sociale	Economico Finanziario, Lavori Pubblici e Manutenzioni, Affari Generali, Edilizia Privata	Server, Personal computer e archivi cartacei
3	Dati idonei a rivelare sieropositività	SI		Assistenza Sociale		Server, Personal computer e archivi cartacei
4	Dati idonei a rivelare malattie infettive e diffusive	SI		Assistenza Sociale	Polizia Locale, Lavori Pubblici e Manutenzioni	Server, Personal computer e archivi cartacei
5	Dati idonei a rivelare malattie mentali	SI		Assistenza Sociale	Economico Finanziario, Affari Generali, Polizia Locale	Server, Personal computer e archivi cartacei
6	Dati idonei a rivelare lo stato di salute	SI		Assistenza Sociale, Economico Finanziario, Affari Generali	Centro Diurno Anziani, Gruppo Sportivo ARS	Server, Personal computer e archivi cartacei
7	Dati relativi a prescrizioni farmaceutiche e cliniche	SI		Assistenza Sociale, Economico Finanziario, Affari Generali		Server, Personal computer e archivi cartacei
8	Dati relativi ad esiti diagnostici e programmi terapeutici	SI		Assistenza Sociale, Economico Finanziario, Affari Generali		Server, Personal computer e archivi cartacei
9	Dati relativi all'utilizzo di particolari ausili protesici	SI		Assistenza Sociale, Economico Finanziario, Affari Generali		Server, Personal computer e archivi cartacei
10	Dati relativi alla prenotazione di esami clinici e visite specialistiche	SI		Assistenza Sociale, Economico Finanziario, Affari Generali		Server, Personal computer e archivi cartacei
11	Dati idonei a rivelare AIDS conclamato	SI		Assistenza Sociale		Server, Personal computer e archivi cartacei
12	Dati giudiziari		SI	Affari Generali, Economico Finanziario, Lavori Pubblici e Manutenzioni, Edilizia Privata, Assistenza Sociale, Polizia Locale		Server, Personal computer e archivi cartacei

13	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche			Affari Generali, Economico Finanziario, Lavori Pubblici e Manutenzioni, Edilizia Privata, Assistenza Sociale, Polizia Locale	Centro Diurno Anziani, Gruppo Sportivo ARS, Lombardia Nuoto SSD a r.l. di Monza	Server, Personal computer e archivi cartacei
14	Dati idonei a rivelare convinzioni di altro genere (diverse da religiose o filosofiche)	SI		Assistenza Sociale, Affari Generali	Sodexo Italia S.p.A. di Cinisello Balsamo	Server, Personal computer e archivi cartacei
15	Dati idonei a rivelare gusti, preferenze, abitudini di vita o di consumo			Assistenza Sociale, Affari Generali		Server, Personal computer e archivi cartacei
16	Dati idonei a rivelare l'adesione a partiti	SI		Affari Generali	Economico Finanziario	Server, Personal computer e archivi cartacei
17	Dati idonei a rivelare l'adesione a sindacati	SI		Affari Generali	Economico 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		Assistenza Sociale, Affari Generali, Economico Finanziario		Server, Personal computer e archivi cartacei
19	Dati idonei a rivelare le convinzioni filosofiche	SI		Assistenza Sociale, Affari Generali		Server, Personal computer e archivi cartacei
20	Dati idonei a rivelare le convinzioni religiose	SI		Assistenza Sociale, Affari Generali	Sodexo Italia S.p.A. di Cinisello Balsamo	Server, Personal computer e archivi cartacei
21	Dati idonei a rivelare le opinioni politiche	SI		Assistenza Sociale, Affari Generali		Server, Personal computer e archivi cartacei
22	Dati idonei a rivelare lo stato matrimoniale o di famiglia			Assistenza Sociale, Affari Generali		Server, Personal computer e archivi cartacei
23	Dati idonei a rivelare l'origine nazionale	SI		Assistenza Sociale, Affari Generali		Server, Personal computer e archivi cartacei
24	Dati idonei a rivelare l'origine razziale ed etnica	SI		Assistenza Sociale, Affari Generali	Sodexo Italia S.p.A. di Cinisello Balsamo	Server, Personal computer e archivi cartacei
25	Dati relativi a comportamenti illeciti o fraudolenti		SI	Polizia Locale, Assistenza Sociale	Affari Generali, Lavori Pubblici e Manutenzioni, Edilizia Privata	Server, Personal computer e archivi cartacei
26	Dati relativi ad altri provvedimenti o procedimenti giudiziari		SI	Polizia Locale, Assistenza Sociale, Edilizia Privata, Lavori Pubblici e Manutenzioni, Affari Generali		Server, Personal computer e archivi cartacei
27	Dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili		SI	Polizia Locale, Affari Generali, Assistenza Sociale, Economico Finanziario		Server, Personal computer e archivi cartacei
28	Dati relativi al comportamento debitorio			Economico Finanziario, Affari Generali		Server, Personal computer e archivi cartacei
29	Dati relativi al grado di istruzione o di cultura			Affari Generali, Assistenza Sociale		Server, Personal computer e archivi cartacei
30	Dati relativi alle pregresse esperienze professionali			Affari Generali, Economico Finanziario, Lavori Pubblici e Manutenzioni, Edilizia Privata, Assistenza Sociale, Polizia Locale		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)			Affari Generali, Economico Finanziario, Lavori Pubblici e Manutenzioni, Edilizia Privata, Assistenza Sociale, Polizia Locale	dott. Gianluca GROSSI di Torrile (PR)	Server, Personal computer e archivi cartacei
32	Dati idonei a rivelare l'appartenenza a categorie protette	SI		Affari Generali, Assistenza Sociale		Server, Personal computer e archivi cartacei
33	Dati idonei a rivelare lo stato di gravidanza	SI		Affari Generali, Assistenza Sociale		Server, Personal computer e archivi cartacei
34	Dati relativi ad eventuali controversie con precedenti datori di lavoro		SI	Affari Generali		Server, Personal computer e archivi cartacei
35	Gestione archivio comunale	SI	SI	Affari Generali	Aruba S.p.A.	Server, Personal computer e archivi cartacei
36	Gestione albo pretorio e notifiche		SI	Affari Generali		Server, Personal computer e archivi cartacei
37	Gestione anagrafe della popolazione residente in Italia e all'estero e relativi adempimenti	SI	SI	Affari Generali		Server, Personal computer e archivi cartacei
38	Gestione stato civile della popolazione residente e relativi adempimenti	SI	SI	Affari Generali		Server, Personal computer e archivi cartacei
39	Gestione schedario elettorale e relativi fascicoli	SI		Affari Generali		Server, Personal computer e archivi cartacei
40	Aggiornamento elenco giudici popolari		SI	Affari Generali		Server, Personal computer e archivi cartacei
41	Gestione del personale dipendente dell'ente e relativi adempimenti	SI	SI	Affari Generali, Economico Finanziario		Server, Personal computer e archivi cartacei
42	Gestione assicurazioni dell'ente	SI	SI	Affari Generali	Assiteca S.p.A. di Milano	Server, Personal computer e archivi cartacei
43	Gestione procedimenti di spesa e di entrata			Economico Finanziario	dott. Gianluca GROSSI di Torrile (PR)	Server, Personal computer e archivi cartacei
44	Riscossioni di tributi e imposte diverse			Economico Finanziario	Studio K s.r.l. di Reggio Emilia, Aletti Impianti s.r.l. di Bisuschio, Prealpi Servizi s.r.l. di Varese, Cooperativa sociale Fraternità Sistemi Onlus di Brescia	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	Assistenza Sociale, Affari Generali, Economico Finanziario, Lavori Pubblici e Manutenzioni, Edilizia Privata, Polizia Locale		Server, Personal computer e archivi cartacei
46	Gestione procedimenti in materia di polizia amministrativa (autorizzazione, licenze, permessi, ecc.)		SI	Polizia Locale		Server, Personal computer e archivi cartacei
47	Procedimenti connessi all'applicazione del codice della strada (contravvenzioni, infrazioni, rilevazioni incidenti stradali)	SI	SI	Polizia Locale		Server, Personal computer e archivi cartacei
48	Acquisizione denunce d'infortunio	SI		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	Assistenza Sociale, Affari Generali, Economico Finanziario		Server, Personal computer e archivi cartacei
50	Attività inerenti la biblioteca comunale	SI		Affari Generali		Server, Personal computer e archivi cartacei
51	Gestione pratiche per il rilascio concessioni edilizie o autorizzazioni			Lavori Pubblici e Manutenzioni, Edilizia Privata		Server, Personal computer e archivi cartacei

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 dati trattati sono registrati in banche dati memorizzate nel server principale situato in un locale presso la sede Municipale di Via Cavour, 37 e sono gestiti dagli incaricati del trattamento attraverso personal computer collegati tramite ethernet 100 Mb o fibra ottica per le sedi remote.
Oltre alle copie di Backup presenti presso la sede comunale, è presente un ulteriore sistema di backup basato su un server dedicato in ambiente Unix (Secure Box), controllato quotidianamente dall'Amministratore di sistema.

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

- Via Cavour, 37
- Biblioteca Comunale, Via Pompeo Marchesi, 16

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	1	0	0
B3	2	0	0
C	6	0	0
D1	4	0	0

- Servizi in convenzione:
a) Servizio Sociale con il Comune di Clivio (VA)
b) gestione del servizio acquedotto con i Comuni di Viggiù e Clivio (Saltrio comune capo convenzione)
c) servizio bibliotecario Valli dei Mulini (41 comuni coinvolti, comune capo convenzione Malnate)
d) convenzione di segreteria per il segretario comunale (comune capo convenzione Cuveglio, 5 comuni coinvolti)
e) convenzione gestione della scuola secondaria Via Molino dell'Olio Saltrio e della direzione dell'Istituto comprensivo Via Indipendenza Viggiù con i Comuni di Viggiù e Clivio (Saltrio comune capo convenzione)
f) Convenzione ex art. 30 Tuel per la gestione in forma associata dei sistemi informativi dei Comuni della Comunità Montana Piambello
g) Convenzione ex art. 30 Tuel relativa al servizio di ricovero di animali di affezione con la Comunità Montana Piambello
h) Convenzione ex art. 30 Tuel relativa allo Sportello unico per le attività produttive - S.U.A.P. con la Comunità Montana Piambello
i) Convenzione ex art. 30 Tuel in materia di raccolta dei funghi epigei con la Comunità Montana Piambello

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

- Affari Generali
- Assistenza Sociale
- Economico Finanziario
- Edilizia Privata
- Lavori Pubblici e Manutenzioni
- Polizia Locale

In data 12.03.2010 il Sindaco, nella sua qualità di Titolare del trattamento, comunicava la designazione a incaricato del trattamento dei dati a tutto il personale dipendente, ogni qualvolta il dipendente accede alla banche dati gestite dal Comune di Saltrio.

Ditta	Trattamento	Inizio mandato	Fine mandato
Aletti Impianti s.r.l. di Bisuschio	Servizio di manutenzione acquedotto Viggiù Saltrio Clivio e prestazioni complementari		
Aruba S.p.A.	Conservazione digitale		
Assiteca S.p.A. di Milano	Servizio professionale di brokeraggio assicurativo		
BF s.r.l. di Busto Arsizio	Centralino telefonico digitale		
Banca Popolare di Sondrio S.C.p.A. – sede centrale di Sondrio – filiale di Viggiù	Servizio di tesoreria comunale		
Centro Diurno Anziani	Associazione Centro Diurno Anziani		

Cooperativa sociale Fraternità Sistemi Onlus di Brescia	Riscossione dei tributi		
DUECI s.n.c. di Gallarate	Manutenzione hardware della rete informatica comunale		
Econord S.p.A. di Varese	Servizio di igiene urbana		
Filarmonica Saltriese	Associazione		
Gruppo Sportivo ARS	Associazione Gruppo Sportivo ARS		
Gruppo volontari di antincendio e protezione civile	Associazione Gruppo volontari di antincendio e protezione civile		
Lombardia Nuoto SSD a r.l. di Monza	Gestione centro sportivo comunale in Via Rossini		
Prealpi Servizi s.r.l. di Varese	Servizio di analisi acqua potabile e Servizio di lettura e fatturazione dei consumi di acqua potabile, fognatura, depurazione comuni Viggiù Saltrio Clivio e servizio sportello		
Progetti di Impresa s.r.l. di Modena	Gestione sito comunale		
S.I.E.M. di Mancastroppa Giuseppe & C. s.n.c. di Cremona	Concessione gestione impianto elettrico votivo del cimitero comunale		
Sodexo Italia S.p.A. di Cinisello Balsamo	Servizio di ristorazione scuolastica		
Studio K s.r.l. di Reggio Emilia	Manutenzione hardware e software della rete informatica comunale		
dott. Gianluca GROSSI di Torrile (PR)	Revisore dei conti		

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**
Affari Generali	Salvatore RICCIO	6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 45, 49, 50	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

Assistenza Sociale	dott.ssa Solidea PERONI	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 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
Economico Finanziario	rag. Antonella BERNASCONI	6, 7, 8, 9, 10, 12, 13, 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
Edilizia Privata	geom. Giuseppe FRANZI (Vice Sindaco, Assessore e Consigliere)	12, 13, 26, 30, 31, 45, 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
Lavori Pubblici e Manutenzioni	geom. Giuseppe FRANZI (Vice Sindaco, Assessore e Consigliere)	12, 13, 26, 30, 31, 45, 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

Polizia Locale	Ing. Maurizio ZANUSO (Sindaco)	12, 13, 25, 26, 27, 30, 31, 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

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 dell'ente e comunque tutti gli immobili nei quali sono posizionati i personal computer collegati al server sono dotati di un sistema di sicurezza. L'accesso ai database è assicurato da password.
Sul territorio comunale è presente un sistema di videosorveglianza gestito da un regolamento approvato nel Settembre 2011.

Nell'edificio il server è posizionato in un locale chiuso a cui ha accesso unicamente il responsabile del sistema informativo e il personale autorizzato.

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 anche irreparabili	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
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	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

	comportamento fraudolento		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 software informatici gli hackers sono in grado di inviare documenti utilizzando il vostro indirizzo e-mail	3	Adozione di programmi 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	6	Assicurare la manutenzione ordinaria attraverso appositi contratti manutentivi, Provvedere alla sostituzione delle apparecchiature al fine di

	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.		prevenire il degrado o l'indisponibilità degli strumenti
Accessi esterni non autorizzati	Qualsiasi forma di intrusione dall'esterno al sistema informatico arreca danni alle banche dati creando notevoli disagi e problemi a tutta la struttura	4	Adozione di sistemi firewall, con relativo aggiornamento periodico
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 possibili	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)
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	Dare attuazione ai corsi di formazione previsti per gli apicali dell'ente e per tutto il personale così come previsto nell'apposita sezione del presente DPS		Annuale o al momento dell'assunzione	Amministratore di Sistema, Affari Generali
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	Amministratore di Sistema, Affari Generali
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	Installare appositi software che impediscano ai dipendenti l'utilizzo di programmi non autorizzati.		Aggiornamento Trimestrale dei software	Amministratore di Sistema, Affari Generali
Attribuire la custodia dei software e delle relative licenze al responsabile	Evitare che i software vengano utilizzati da dipendenti per fini personali	Nessuna	Nessuna	In essere	Effettuare l'atto di attribuzione della responsabilità al responsabile		Una tantum	Affari Generali
Installazione e aggiornamenti programmi antivirus	Evitare l'intrusione di virus nel sistema	Tutti	Tutte	In essere			Aggiornamento almeno settimanale	Amministratore di Sistema, Affari Generali
Informazione ai dipendenti del divieto di installare programmi non autorizzati	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	Affari Generali

suscettibili di recare danni alle banche dati dell'ente								
Installazione e aggiornamenti programmi antispamming	Evitare la saturazione inutile delle caselle e-mail con il rischio di importare virus	Tutti	Tutte	In essere	Acquistare e installare appositi software		Aggiornamento Mensile	Amministratore di Sistema, Affari Generali
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	Acquistare e installare appositi software		Aggiornamento Mensile	Amministratore di Sistema, Affari Generali
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	Acquistare e installare appositi software e sviluppare l'uso della firma digitale		Aggiornamento Trimestrale	Amministratore di Sistema, Affari Generali
Disabilitare la risposta al ping sul firewall	Evitare che la linea ADSL sia satura e resa inutilizzabile dagli hacker	Nessuna	Nessuna	In essere	Attivare l'apposita funzione		Una Tantum	Amministratore di Sistema, Affari Generali
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	Affari Generali, Economico Finanziario
Prevedere la sostituzione dell'hardware all'occorrenza con estrema sollecitudine	La sostituzione dell'hardware permette di avere un sistema informatico sempre all'avanguardia ed in grado di assicurare il migliore trattamento dei dati possibile	Tutti	Tutte	In essere	Dotarsi di appositi contratti che prevedano una celere sostituzione degli strumenti qualora si renda necessario		Biennale	Affari Generali, Responsabile Esterno
Evitare l'accesso ai locali da parte di personale non autorizzato	Evitare la diffusione di dati	Tutti	Tutte	In essere	Formare il personale al fine di renderlo edotto dei possibili rischi derivanti		Una tantum o al momento dell'assunzione	Affari Generali, Ogni Responsabile di Area
Dotare le apparecchiature informatiche di idonei sistemi di sicurezza (password, crittografia) 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 semestrale, Cavetto di sicurezza: una tantum ed all'occorrenza, Circolare al personale: una tantum	Affari Generali, Ogni dipendente
Accertare il funzionamento dei sistemi di allarme degli uffici	Evitare l'ingresso di estranei al di fuori degli orari consentiti	Tutti	Tutte	In essere	Dotare di sistema di allarme la sede dell'Ente		Verifica semestrale del regolare funzionamento	Affari Generali, Lavori Pubblici e Manutenzioni

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				Amministratore di Sistema, Affari Generali
Depositare copia dei backup in luogo esterno alla struttura (es. cassetta di sicurezza in banca)	Evitare che in caso di danni alla struttura vengano persi definitivamente tutti i dati	Tutti	Tutte	In essere	Incaricare un soggetto che porti nella sede indicata la copia dei dati almeno una volta settimana		Una Tantum	Amministratore di Sistema, Affari Generali
Dotare l'ente di una apposita linea elettrica dedicata	Evitare che ci siano sovraccarichi nell'impianto elettrico dell'ente causando disguidi nel funzionamento delle apparecchiature	Tutti	Tutte	In essere	Richiedere all'ente erogatore dell'energia elettrica tale linea		Una Tantum	Affari Generali, Responsabile Esterno
Dotare l'ente di gruppi di continuità	Consentire che in caso di guasti alla rete elettrica o in caso di interruzione della somministrazione dell'energia sia possibile effettuare almeno il salvataggio dei dati	Tutti	Tutte	In essere			Trimestralmente verificare il funzionamento	Affari Generali, Amministratore di Sistema
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	Affari Generali, Lavori Pubblici e Manutenzioni

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 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. 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.

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 per la salvaguardia dei dati	Tutti i dipendenti	Tutti	Tutti devono essere formati	Tra l'anno 2014 e l'anno 2015 la Comunità Montana del Piambello ha organizzato, per tutti i Comuni facenti parte dalla Comunità Montana, una serie di incontri finalizzati alla presentazione delle funzioni ricoperte dall'Amministratore di Sistema e di tutte le misure di sicurezza da adottare presso il singolo Ente, secondo quanto riportato nell'allegato B del D.Lgs. 196/2003.

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 manutenzione acquedotto Viggiù Saltrio Clivio e prestazioni complementari	Servizio di manutenzione acquedotto Viggiù Saltrio Clivio e prestazioni complementari	Non vengono trattati dati sensibili	Aletti Impianti s.r.l. di Bisuschio
Conservazione digitale	Conservazione digitale	La ditta viene a contatto con tutte le tipologie di dati	Aruba S.p.A.
Servizio professionale di brokeraggio assicurativo	Servizio professionale di brokeraggio assicurativo	Non vengono trattati dati sensibili	Assiteca S.p.A. di Milano
Centralino telefonico digitale	Centralino telefonico digitale	Non vengono trattati dati sensibili	BF s.r.l. di Busto Arsizio
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 Popolare di Sondrio S.C.p.A. – sede centrale di Sondrio – filiale di Viggiù
Associazione Centro Diurno Anziani	Associazione Centro Diurno Anziani	Potrebbe venire a conoscenza di dati sensibili	Centro Diurno Anziani
Riscossione dei tributi	Riscossione dei tributi	Non vengono trattati dati sensibili	Cooperativa sociale Fraternità Sistemi Onlus di Brescia
Manutenzione hardware della rete informatica comunale	Manutenzione hardware della rete informatica comunale	Gestendo la rete la ditta viene a contatto con tutte le tipologie di dati	DUECI s.n.c. di Gallarate
Servizio di igiene urbana	Servizio di igiene urbana	Non vengono trattati dati sensibili	Econord S.p.A. di Varese
Associazione	Associazione	Non vengono trattati dati sensibili	Filarmonica Saltriese
Associazione Gruppo Sportivo ARS	Associazione Gruppo Sportivo ARS	Potrebbe venire a conoscenza di dati sensibili	Gruppo Sportivo ARS
Associazione Gruppo volontari di antincendio e protezione civile	Associazione Gruppo volontari di antincendio e protezione civile	Potrebbe venire a conoscenza di dati sensibili	Gruppo volontari di antincendio e protezione civile
Gestione centro sportivo comunale in Via Rossini	Gestione centro sportivo comunale in Via Rossini	Potrebbe venire a conoscenza di dati sensibili	Lombardia Nuoto SSD a r.l. di Monza
Servizio di analisi acqua potabile e Servizio di lettura e fatturazione dei consumi di acqua potabile, fognatura, depurazione comuni Viggiù Saltrio Clivio e servizio sportello	Servizio di analisi acqua potabile e Servizio di lettura e fatturazione dei consumi di acqua potabile, fognatura, depurazione comuni Viggiù Saltrio Clivio e servizio sportello	Non vengono trattati dati sensibili	Prealpi Servizi s.r.l. di Varese
Gestione sito comunale	Gestione sito comunale	La ditta viene a contatto con tutte le tipologie di dati	Progetti di Impresa s.r.l. di Modena
Concessione gestione impianto elettrico votivo del cimitero comunale	Concessione gestione impianto elettrico votivo del cimitero comunale	Non vengono trattati dati sensibili	S.I.E.M. di Mancastroppa Giuseppe & C. s.n.c. di Cremona
Servizio di ristorazione scolastica	Preparazione pasti per alunni e personale delle scuole materne, elementari e medie	L'azienda viene a conoscenza delle patologie degli alunni e delle abitudini alimentari dei medesimi	Sodexo Italia S.p.A. di Cinisello Balsamo
Manutenzione hardware e software della rete informatica comunale	Manutenzione hardware e software della rete informatica comunale	Gestendo la rete la ditta viene a contatto con tutte le tipologie di dati	Studio K s.r.l. di Reggio Emilia
Revisore dei conti	Revisore dei conti	Non vengono trattati dati sensibili	dott. Gianluca GROSSI di Torrile (PR)

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.