Approvato con deliberazione della Giunta Municipale
n. 26 del 30 marzo 2011.
Il Segretario comunale Pierfilippo Fattori
Il Sindaco pro-tempore Rinaldo De Rocco

COMUNE DI CANALE D'AGORDO (BL)

Documento programmatico sulla sicurezza dei dati

Redatto in base alle disposizione di cui al punto 19 del
DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA
del CODICE IN MATERIA DI DATI PERSONALI
(Dls. n. 196 del 30 giugno 2003)

ANNO 2011

1. Indice

2. Documento programmatico sulla sicurezza dei dati

Redatto in base alle disposizione di cui al punto 19 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del CODICE IN MATERIA DI DATI PERSONALI (D.lgs. n.196 del 30 giugno 2003)

2.1. Revisione

Il presente documento rivede e sostituisce il precedente documento programmatico sulla sicurezza dei dati, approvato con deliberazione della Giunta Comunale n.120 del 19 dicembre 2005.

2.2. Scopo

Da sempre il diritto alla riservatezza dell'individuo subisce limitazioni dovute alla necessità di vari soggetti, privati e pubblici, di acquisire informazioni necessarie per lo svolgimento di attività istituzionali. Ma oggi lo sviluppo tecnologico e l'evoluzione delle reti telematiche espongono il singolo individuo ad un rischio di violazione della sfera privata e del diritto alla riservatezza ben maggiore che in passato.

Per fare fronte a questo fenomeno la legge 31 dicembre 1996, n. 675, dando attuazione alla Direttiva europea 95/46/CE, ha disciplinato per la prima volta in modo più preciso questa materia.

In seguito, nel 2003 è stato emanato il Decreto legislativo 30 giugno 2003, n. 196, contenente il Codice in materia di protezione dei dati personali, che integra ed aggiorna tale normativa.

Tale legge disciplina in particolare la protezione di diritti riconosciuti come inviolabili e fondamentali della persona dell'art. 2 della Costituzione, quali:

il diritto alla riservatezza, vale a dire il diritto che ognuno può esercitare per mantenere libera da ingerenze esterne la propria vita privata.

Il diritto all'identità personale, che è il diritto che ogni individuo può esercitare per utilizzare in esclusiva il proprio nome e altri elementi identificativi della propria persona.

L'Amministrazione comunale ha ritenuto di adeguarsi alla complessa normativa in materia di privacy. Si è quindi proceduto ad una accurata analisi della situazione esistente in materia di tutela dei dati personali e delle misure di sicurezza già attuate presso le varie strutture comunali, arrivando infine a realizzare il presente documento che vuole essere uno strumento operativo a disposizione dei vari soggetti che assumono ruoli di responsabilità, direttivi ed operativi, nel trattamento dei dati personali.

L'obiettivo principale è quello di fornire una precisa fotografia della situazione esistente in materia di sicurezza, fornendo al contempo utili indicazioni pratiche in ordine alle varie misure (organizzative, procedurali, tecniche e logistiche) applicate, da applicare o da migliorare per ridurre la probabilità di danni e garantire un sufficiente livello di sicurezza delle banche dati gestite dall'Amministrazione comunale.

Il presente DPS, escludendo la prima parte contenente le definizioni e i punti principali della legge, è stato redatto partendo dalla bozza di schema rilasciata dal garante in data 13 maggio 2004 e apportandovi delle modifiche per una miglior contestualizzazione alla realtà specifica del Comune di Canale d'Agordo.

2.3. Ambito di applicazione

Il Documento Programmatico Sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda il trattamento di tutti i dati personali:

Sensibili

Giudiziari

Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali per mezzo di:

Strumenti elettronici di elaborazione

Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il Documento programmatico sulla sicurezza deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

2.4. Riferimenti normativi

CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003)
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice) ed allegato B.

2.5. Definizioni

2.5.1. Definizione di dati personali

Dato personale è qualunque informazione (e non solo quelle di carattere riservato) che consenta di individuare con certezza un soggetto in modo diretto o indiretto, vale a dire anche quando l'identificazione sia possibile attraverso il collegamento di più informazioni di per sé non significative se singolarmente considerate. Il Codice definisce come dati identificativi i dati immediatamente associati ad una persona determinata, e i dati identificabili come i dati che non essendo immediatamente associati a persone determinate necessitano di un "ragionevole sforzo" per essere conosciuti.
Il Codice individua, tra i dati personali, le seguenti categorie: dati sensibili, dati giudiziari, altri dati particolari, dati comuni.
Questa classificazione è stabilita in funzione del diverso livello di riservatezza intrinseco alle varie tipologie di dati, delle diverse precauzioni che la legge richiede per il loro utilizzo, per la loro custodia e per il loro trattamento e della oggettiva diversa pericolosità per l'individuo derivante da un eventuale illecito trattamento.

2.5.2. Definizione di dati sensibili

Sono i dati personali individuati dall'art. 4, comma 1, lettera d, del Codice, 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 o organizzazioni a carattere religioso, filosofico, politico o sindacale; lo stato di salute e la vita sessuale.
La definizione di dato sensibile è esclusiva: sono considerati tali solo i dati specificamente indicati, indipendentemente dal carattere di riservatezza o di particolare rilevanza che un individuo, o il senso comune, può attribuire ad altre tipologie di dati (ad esempio: codice identificativo della carta di credito, reddito, stato di separazione ecc.).
A tutela della sicurezza dei dati sensibili sono imposte misure particolarmente rigide che sono illustrate nel presente documento, sia per quanto riguarda i presupposti di legittimazione al trattamento e alla comunicazione e diffusione sia con riferimento alle misure tecniche, organizzative e logistiche da adottare per il loro trattamento e per la loro conservazione.

2.5.3. Definizione di dati giudiziari

Sono i dati personali indicati dall'articolo 4, comma 1, lettera e, del Codice, idonei a rivelare provvedimenti di cui all'articolo 686, commi l, lettere a) e d), 2 e 3, del Codice di procedura penale. Riguardano le iscrizioni al casellario giudiziario in materia penale quali ad esempio: condanna penale, dichiarazione di abitualità nel reato, pene accessorie ecc. Anche tali dati sono tutelati, sotto il profilo della sicurezza, con apposite misure organizzative e gestionali.

2.5.4. Definizione degli altri dati particolari

Si tratta di un'ulteriore categoria prevista dall'articolo 17 del Codice, intermedia tra dati sensibili e comuni, il cui trattamento presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. Il loro trattamento è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato ove prescritti dal Garante.

2.5.5. Definizione di dati comuni

Sono tutti i restanti dati personali, non compresi nelle precedenti categorie.

2.5.6. Definizione di banca dati

È qualsiasi insieme di dati personali organizzati in modo da renderne possibile o agevole la consultazione e il trattamento.
Non si considerano, pertanto, le sole "raccolte" informatizzate, bensì tutte le raccolte di dati personali, a prescindere dallo strumento usato per il trattamento dei dati, comprendendo anche strumenti di archiviazione quali i supporti audiovisivi, ottici, fotografici e le "raccolte" cartacee. Ai fini dell'applicazione delle misure di sicurezza, sono rilevanti non solo le banche dati ufficiali, ma anche le semplici raccolte di dati personali finalizzate all'ordinaria gestione dell' attività amministrativa.

2.5.7. Definizione di trattamento di dati personali

Costituisce un trattamento di dati personali (art. 4 lettera a del Codice) qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, 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.
La riservatezza dei dati è sempre tutelata indipendentemente dalle modalità di gestione (manuale o con strumenti elettronici).

2.5.8. Definizioni di comunicazione e di diffusione

La comunicazione è operazione di trattamento che consiste nel portare dati personali a conoscenza di uno o più soggetti determinati (identificabili in modo univoco e determinato), diversi dall'interessato cui i dati stessi si riferiscono, in qualunque forma, anche mediante la loro messa a disposizione per la consultazione.
Non si considera comunicazione lo scambio di dati tra strutture interne dell'amministrazione o tra queste ultime e soggetti esterni individuati come responsabili o incaricati del trattamento nell'ambito di attività di outsourcing o in base ad atto convenzionale (ad es.: affidamento all'esterno di compiti dell'amministrazione). In tal caso anche i soggetti esterni che collaborano con il Comune vengono considerati "articolazioni" dello stesso.
La diffusione è operazione di trattamento che consiste nel portare dati personali a conoscenza di soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione per la consultazione.
Tipica forma di diffusione è quella che si realizza tramite registri o albi pubblici ovvero con la pubblicazione delle deliberazioni e determinazioni.

2.6. Presupposti che legittimano il trattamento dei dati personali da parte della pubblica amministrazione

Ai sensi dell' art. 18 del Codice, il trattamento di dati personali da parte dei soggetti pubblici, esclusi gli enti pubblici economici (il cui regime è equiparato a quello dei privati) è consentito soltanto:
per lo svolgimento delle funzioni istituzionali
nei limiti dettati da leggi e regolamenti.
Pertanto, di fronte a qualsiasi trattamento, il responsabile del trattamento stesso (dirigente) deve verificare:
che il trattamento sia connesso con l'esercizio delle funzioni istituzionali e che le stesse finalità non siano perseguibili attraverso il trattamento di dati anonimi (principio di pertinenza);
che le modalità del trattamento siano tali da determinare il minimo sacrificio possibile del diritto alla riservatezza dei terzi (principio di non eccedenza);
che il trattamento ed in particolare le modalità adottate non siano difformi alle norme di legge e di regolamento;
che vengano adottate le misure di sicurezza.
Come tutti i soggetti, anche le amministrazioni pubbliche devono applicare quanto previsto dall'articolo 3 del Codice (principio di necessità). I sistemi informativi e i programmi informatici vanno configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le

finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
Anche quando l'amministrazione persegue finalità istituzionali mediante gli strumenti del diritto privato (disciplina del rapporto di lavoro, attività contrattuale, ecc.) ai fini della normativa sulla protezione dei dati personali essa è comunque da considerarsi soggetto pubblico, avendo rilevanza l'aspetto soggettivo della stessa e non la natura dei rapporti gestiti.

2.6.1. Trattamento di dati personali da parte della pubblica amministrazione senza la necessità del consenso dell'interessato

In presenza dei presupposti giuridici illustrati al punto precedente, la pubblica amministrazione può legittimamente trattare dati personali senza acquisire il consenso dell'interessato. Al contrario, l'acquisizione del consenso dell'interessato non legittima l'amministrazione a trattare dati per finalità diverse da quelle istituzionali o a effettuare operazioni non consentite da leggi o regolamenti. Nei confronti della pubblica amministrazione, il consenso pertanto non rimuove il limite dato dalla mancanza dei presupposti che legittimano il trattamento.

2.6.2. Presupposti che legittimano la comunicazione e la diffusione dei dati personali da parte dei soggetti pubblici

La disciplina si differenzia a seconda del soggetto destinatario.

Comunicazione o diffusione a soggetti pubblici: la comunicazione e la diffusione a soggetti pubblici, esclusi gli enti pubblici economici, dei dati trattati sono ammesse (art. 19 del Codice) quando siano previste da norme di legge o di regolamento o quando risultino comunque necessarie per lo svolgimento delle funzioni istituzionali; in questo caso, mancando una disposizione normativa o regolamentare, va data previa comunicazione al Garante, che può vietare tale operazione qualora risultino violate disposizioni di legge.

Comunicazione o diffusione a privati o enti pubblici economici: la comunicazione e la diffusione dei dati personali da parte di soggetti pubblici a privati o a enti pubblici economici sono ammesse solo quando siano previste da norme di legge o di regolamento (art. 19, comma 3, del Codice).

Diffusione dei dati relativi allo stato di salute: esiste un generale divieto di diffusione dei dati relativi allo stato di salute, salvo per i motivi di prevenzione, accertamento e repressione dei reati.

2.6.3. La notifica dei trattamenti

Mentre secondo la normativa precedente la notificazione era sempre obbligatoria salvo eccezioni, secondo il nuovo codice il titolare deve notificare al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:
a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
d) dati trattati con l' ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Poiché l'organizzazione del Comune può essere articolata, sono i responsabili dei trattamenti (segretario comunale e titolari di posizione organizzativa) che devono verificare se i trattamenti che si svolgono sotto la loro responsabilità appartengono ad una delle categorie soggette a notifica, per adempiere a questo obbligo predisponendo l'atto di notifica al Garante da far trasmettere al Sindaco in qualità di rappresentante del titolare.

2.7. Adempimenti riguardo le misure di sicurezza

Le misure di sicurezza sono costituite dal complesso delle misure organizzative, tecniche, informatiche, logistiche e procedurali volte a ridurre al minimo i rischi di:
distruzione o perdita, anche accidentale dei dati,
accesso non autorizzato;
trattamento non consentito o non conforme alle finalità della raccolta
modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole
Tutti i titolari sono tenuti ad adottare misure minime individuate dal Codice e secondo le modalità previste nel Disciplinare tecnico allegato al Codice. Va sottolineato come l'articolo 31 del Codice non fa differenza tra violazione della riservatezza dei dati personali propriamente detta - quale si avrebbe ad esempio nel caso di accesso a dati sensibili da parte di terzi non autorizzati - e distruzione o perdita accidentale di dati già legittimamente raccolti e trattati. La mancata custodia dei dati è comunque causa di un danno, e il responsabile di questo danno è sanzionato. Infatti dal solo danno della distruzione o perdita dei dati derivano varie gravi conseguenze: ad esempio il blocco delle attività, costi gestionali imprevisti, danno di immagine. Inoltre poiché il privato deve poter fare affidamento sui dati che ha già comunicato alla pubblica amministrazione, ne consegue che in caso di negligente custodia egli può richiedere il risarcimento del danno.
Per questi motivi il soggetto che non adotta misure di sicurezza adeguate è sanzionato penalmente (se le misure non rispettano i parametri previsti dal regolamento sulle misure minime secondo le modalità previste dal Disciplinare Tecnico) e può essere chiamato a rispondere civilmente per il risarcimento del danno (se le misure non sono idonee).
Ai sensi dell' art. 31 del Codice, le misure di sicurezza adottate per il trattamento dei dati personali devono essere:
adeguate in relazione alle conoscenze acquisite in base al progresso tecnico e tali da ridurre al minimo i rischi di distruzione dei dati o accesso non autorizzato;
adottate in via preventiva e differenziate in base alla natura dei dati e alle specifiche caratteristiche del trattamento.
La mancata adozione delle misure di sicurezza può dar luogo a responsabilità penale e civile (per il risarcimento dei danni), secondo quanto illustrato nella tabella:

Mancata adozione di	**Conseguenze**	
	Responsabilità Penale	**Responsabilità Civile**
Misure di sicurezza minime	**Si**	**Si**
Misure di sicurezza idonee	**No**	**Si**

In altre parole esistono due diversi livelli di responsabilità. L'Amministrazione deve individuare preventivamente misure di sicurezza che devono almeno rispettare i parametri di sicurezza minimi individuati nel Codice (articoli 33, 34, 35 e 36); se le misure di sicurezza adottate non rispettano i parametri minimi contenuti nel regolamento, scatta la **responsabilità penale.**
Ma l'individuazione di misure che rispettano i parametri previsti come minimi non è sufficiente a liberare da ogni responsabilità il soggetto che effettua il trattamento. Se le misure adottate *non sono idonee ad evitare il danno,* vi può essere comunque la **responsabilità civile,** anche se non ci sono gli estremi per la responsabilità penale prevista dalla legge.

Le conseguenze della mancata adozione di misure di sicurezza sono quindi le seguenti:
la sanzione penale per omessa adozione delle misure minime è quella prevista dall'articolo 169 del Codice (arresto sino a due anni o ammenda da diecimila a cinquantamila euro);

il risarcimento del danno - nel caso le misure adottate non siano idonee ad evitare il danno- è previsto dall'art. 15 legge del Codice che rimanda all'art. 2050 del Codice Civile (relativa allo svolgimento di attività pericolose); in questo tipo di responsabilità è prevista una presunzione speciale di colpa a carico del responsabile del danno (in questo caso chi effettua il trattamento): il responsabile ha l'onere della prova di aver adottato tutto quanto era possibile per evitare il danno, mentre il danneggiato deve solo dimostrare l'esistenza del danno.

E' superfluo ricordare che la mancata applicazione delle misure di sicurezza determinate dal titolare del trattamento (Sindaco quale rappresentante legale del Comune con riferimento alle misure generali, Segretario ed eventualmente responsabile della posizione organizzativa o del servizio competente in materia di informatica per quanto riguarda le ulteriori istruzioni operative integrative) e delle ulteriori indicazioni impartite dal singolo responsabile può dare adito a responsabilità disciplinare.
Poiché il parametro previsto dalla legge per la responsabilità civile è quello dell'idoneità delle misure ad evitare il danno, le misure di sicurezza elencate nel presente documento non rappresentano una limitazione alla adozione da parte dei responsabili di ulteriori misure idonee a garantire livelli di protezione maggiori e più adeguati alle singole situazioni.
Infine va ricordato che le regole concernenti le misure di sicurezza servono anche ad indirizzare il personale ad un utilizzo corretto delle dotazioni informatiche dell'amministrazione, anche ai fini della salvaguardia del patrimonio tecnologico della stessa. Infatti tra le finalità implicite della legge sulla tutela dei dati personali vi è anche il perseguimento di un processo di crescita culturale del personale dell'amministrazione pubblica.

2.8. Misure organizzative comuni a tutti i tipi di trattamento

2.8.1. Disposizioni generali per il trattamento dei dati personali

Ogni trattamento di dati personali è consentito al Comune, in quanto soggetto pubblico, qualora sussistano i presupposti previsti dall'articolo 18 del Codice. Esso deve svolgersi nel rispetto delle seguenti indicazioni:
va privilegiato, ove possibile, il trattamento di dati anonimi;
se non è possibile il perseguimento delle finalità istituzionali mediante il trattamento di dati anonimi, va comunque garantita l'osservanza del principio di necessità, pertinenza e non eccedenza rispetto alle finalità del trattamento medesimo, ai sensi dell' art. 3 del Codice (stretta coerenza con la natura dei compiti da svolgere, minimo utilizzo dei dati personali, adozione di modalità di trattamento il meno lesive possibile).
Inoltre i dati personali devono essere:
trattati in modo lecito e secondo correttezza;
raccolti e registrati per scopi determinati, espliciti e legittimi ed in funzione dello svolgimento di compiti istituzionali, nei limiti stabiliti dalle leggi e dai regolamenti;
esatti e, se necessario, aggiornati;
trattati dagli incaricati del trattamento nominati dal responsabile del trattamento o eventualmente trattati dallo stesso responsabile;
trattati per il tempo strettamente necessario per lo svolgimento dei compiti istituzionali: per tale motivo i documenti e i supporti sui quali sono registrati devono essere archiviati in luogo custodito non appena concluso il trattamento.
Ai fini della sicurezza dei dati personali:
le riproduzioni di documenti equivalgono ai documenti stessi e, pertanto, vanno gestiti con le medesime cautele;
qualunque prodotto dell' elaborazione di dati personali, ancorchè non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, elaborazioni temporanee ecc.), va trattato con le stesse cautele che sarebbero riservate alla versione definitiva.
Le misure individuate nel presente documento si applicano anche ai collaboratori esterni dell'Amministrazione comunale che, nell'ambito dei compiti loro affidati dal Comune, devono procedere al trattamento di dati personali in qualità di responsabili o incaricati del trattamento, come formalmente designati dall' Amministrazione comunale e che utilizzino, per lo svolgimento dei propri compiti, dotazioni informatiche e non informatiche comunali.

2.8.2. Disposizioni speciali per il trattamento dei dati personali sensibili e giudiziari

Il trattamento dei dati sensibili e giudiziari da parte della pubblica amministrazione è soggetto ad una disciplina speciale, individuata, in particolare, dagli articoli 20, 21 e 22 del Codice.

Il trattamento dei dati sensibili e giudiziari:
è consentito solo se autorizzato da un'espressa disposizione di legge, nella quale siano specificati i dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite;
in mancanza di un'espressa disposizione di legge, i soggetti pubblici possono richiedere al Garante l'individuazione delle attività che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato il trattamento dei dati sensibili; il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni con atto di natura regolamentare adottato in conformità al parere espresso dal Garante;
nei casi in cui sia specificata dalla legge o da un provvedimento del Garante la finalità di rilevante interesse pubblico, ma non sono specificati i tipi di dati e le 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 del Codice, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante.

L'articolo 22 del Codice individua i principi applicabili al trattamento dei dati sensibili e giudiziari:
la pubblica amministrazione è autorizzata a trattare esclusivamente i dati sensibili e giudiziari essenziali per lo svolgimento di quelle attività istituzionali che non possono essere adempiute mediante il trattamento di dati anonimi o di dati personali non sensibili. Essa può svolgere le sole operazioni di trattamento strettamente necessarie per il perseguimento delle finalità per le quali il trattamento è consentito (principi di pertinenza e non eccedenza);
nell'informativa di cui all'art. 13 del Codice, l'amministrazione è tenuta ad informare espressamente l'interessato cui i dati sensibili e giudiziari si riferiscono circa le disposizioni legislative che prevedono gli obblighi o i compiti per i quali deve essere eseguito il trattamento e le finalità per cui i dati sono raccolti;
i dati sensibili e giudiziari possono essere comunicati o diffusi nei limiti di quanto previsto da disposizioni di legge o dai provvedimenti assunti ai sensi dell'articolo 20 con atto di natura regolamentare per identificare e rendere pubblici i tipi di dati e di operazioni consentite;
tra i dati sensibili, i dati relativi alla salute non possono essere oggetto di diffusione (comma 8, art. 22);
tra i dati sensibili, per i dati relativi allo stato di salute ed alla vita sessuale vi è l'obbligo di custodia separata rispetto agli altri dati trattati per finalità che non richiedono il loro utilizzo;
sono previste misure di sicurezza particolarmente rigide per il trattamento dei dati sensibili e giudiziari.

3. Elenco dei trattamenti di dati personali

3.1. Scopo

Con riferimento al punto 19.1 dell'allegato B del D.Lgs 196/2003 in questa sezione viene riportato in forma schematica l'elenco completo dei trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati trattati e della struttura interna od esterna che operativamente effettua il trattamento.
Per ogni trattamento si riporta un codice identificato utilizzato nelle successive tabelle al fine di consentire una identificazione univoca e più rapida.

3.2. Elenco dei trattamenti dei dati personali

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati P=Personali S=Sensibili G=Giudiziari	Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Strumenti utilizzati	Eventuali banche dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di interconnessione
1	Atti e registri dello stato civile	PS	Demografico	Comunità Montana Agordina	Cartaceo, Microsoft Office, Ascot web	Banche dati per i programmi citati in strumenti utilizzati	Server locale e server situato presso la sede della Comunità Montana Agordina	Rete locale e intranet
2	Anagrafe della popolazione	PS	Demografico	Comunità Montana Agordina	Cartaceo, Microsoft Office, Ascot web, ANAGAIRE banca dati locale sul pc locale per gli italiani residenti all'estero) è possibile inviare i dati al ministrero degli interni.	Banche dati per i programmi citati in strumenti utilizzati	Server locale e server situato presso la sede della Comunità Montana Agordina	Rete Locale e intranet
3	Elettorale	PG	Demografico	Comunità Montana Agordina	Cartaceo, Microsoft Office, Ascot web	Banche dati per i programmi citati in strumenti utilizzati	Server locale e server situato presso la sede della Comunità Montana Agordina	Rete Locale e intranet
4	Cittadinanza, immigrazione, asilo, condizione dello straniero per rilascio di visti, permessi, attestazioni, autorizzazioni e documenti	PS	Demografico	Comunità Montana Agordina	Cartaceo, Microsoft Office, Ascot web	Banche dati per i programmi citati in strumenti utilizzati	Server locale e server situato presso la sede della Comunità Montana Agordina	Rete Locale e intranet
5	Protocollo	PS	Segreteria	Comunità	Programma	Banche dati per i	Server situato	Intranet

				Montana Agordina	dedicato	programmi citati in strumenti utilizzati	presso la sede della Comunità Montana Agordina	
6	Servizio militare	PS	Demografico	Comunità Montana Agordina	Cartaceo, Microsoft Office, Ascot web	Banche dati per i programmi citati in strumenti utilizzati	Server locale e server situato presso la sede della Comunità Montana Agordina	Rete Locale e intranet
7	Commercio	PS	Demografico		Cartaceo, Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
8	Dati necessari alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari	P	Segreteria		Cartaceo, Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete Locale
9	Gestione dei tributi	P	Att. Economiche, Tributi	Comunità Montana Agordina, DUOMO GPA srl, EQUITALIA NOMOS spa	Cartaceo, Microsoft Office, Ascot web	Banche dati per i programmi citati in strumenti utilizzati	Server locale, server situato presso la sede della Comunità Montana Agordina, archivi presso le società esterne	Rete Locale e intranet
10	Rilascio di contributi finanziamenti elargizioni, attività socio-assistenziali ecc	PS	Ragioneria, Segreteria		Cartaceo, Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
11	Gestione inventari di immobili e mobili	P	Ragioneria, Tecnico	D.O.C. SERVICE srl di Trento	Programma dedicato	Banche dati per i programmi citati in strumenti	Server locale, archivi presso le società esterne	Rete locale

						utilizzati		
12	Lavori pubblici	P	Tecnico	Vari studi di progettazione	Cartaceo, Microsoft Office, Autocad	Banche dati per i programmi citati in strumenti utilizzati	Server locale, archivi presso le società esterne	Rete locale
13	Edilizia privata	P	Tecnico		Cartaceo, Microsoft Office, Programma dedicato (TEC), Autocad	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
14	Dati in materia di Protezione civile	P	Polizia municipale, Tecnico		Cartaceo, Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
15	Dati relativo a fornitori, collaboratori esterni, professionisti, etc	P	Ragioneria, Segreteria, Tecnico, Polizia		Cartaceo,Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
16	Dati relativi al trattamento del lavoro del personale dipendente	PSG	Ragioneria, Segretario Comunale	Comunità Montana Agordina	Cartaceo,Microsoft Office, programma dedicato	Banche dati per i programmi citati in strumenti utilizzati	Server locale, server situato presso la sede della Comunità Montana Agordina	Rete Locale e intranet
17	Delibere	P	Ragioneria, Segreteria, Tecnico, Polizia Segretario Comunale		Cartaceo, Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
18	Determinazioni	P	Ragioneria, Segreteria, Tecnico, Polizia Segretario Comunale		Cartaceo, Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
19	Contratti e convenzioni	PG	Segretario comunale, Tecnico, Ragioneria		Cartaceo, Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
20	Cimitero	P	Tecnico, Polizia		Cartaceo, Microsoft Office	Banche dati per i programmi citati	Server locale	Rete locale

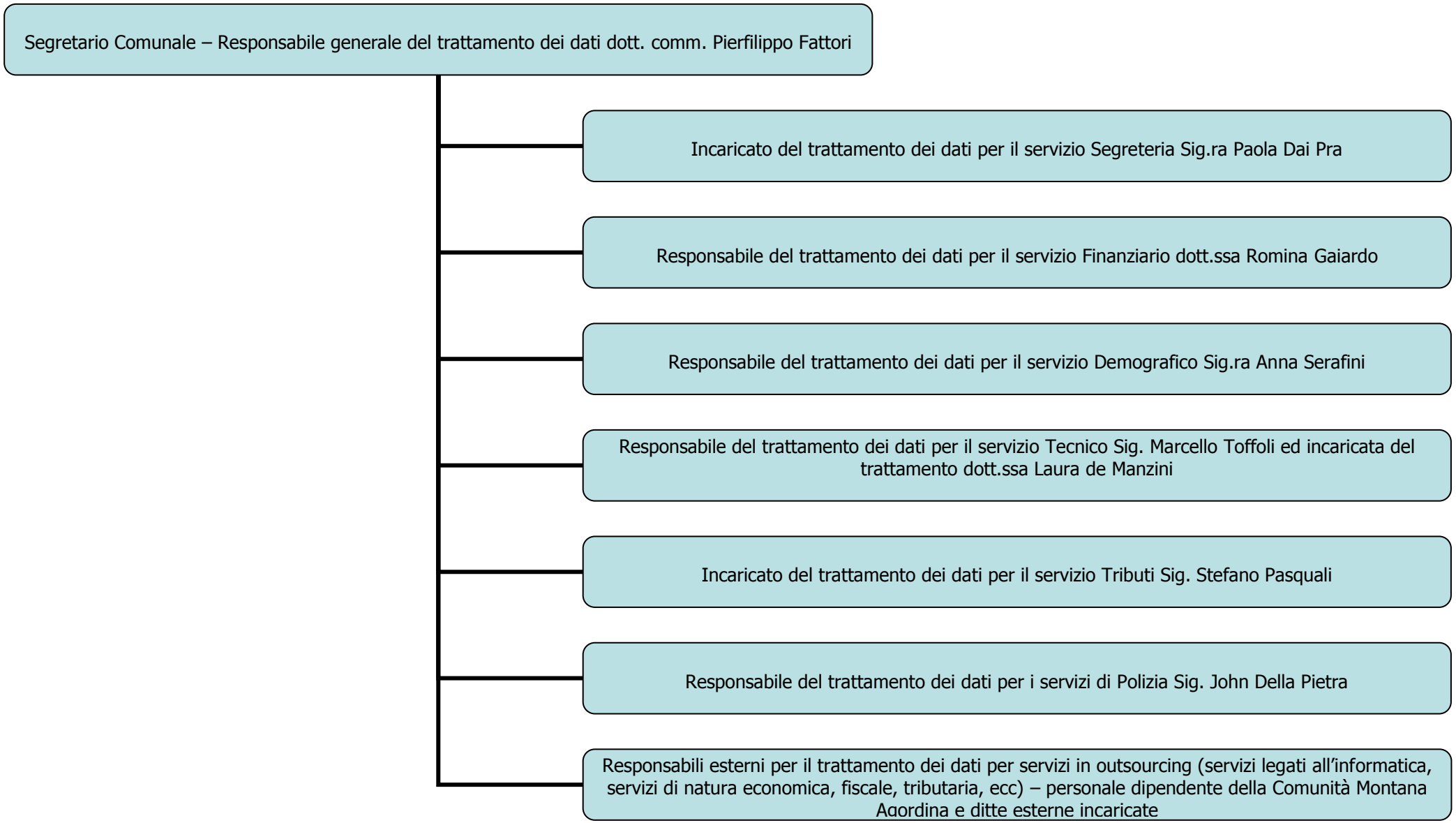
						in strumenti utilizzati		
21	Rapporti con Questura, Procura della Repubblica	PSG	Demografico, Tecnico, Segretario Comunale		Cartaceo, Microsoft Office	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
22	Bilancio	P	Ragioneria		Cartaceo, Microsoft Office, Ascot web	Banche dati per i programmi citati in strumenti utilizzati	Server locale	Rete locale
23	Tesoreria	P	Ragioneria	Cassa Rurale Val di Fassa e Agordino	Cartaceo, Microsoft Office, Ascot web, programma dedicato	Banche dati per i programmi citati in strumenti utilizzati	Server locale, archivi presso le società esterne	Rete locale

4. Distribuzione dei compiti e delle responsabilità

4.1. Scopo

Si riporta di seguito l'organigramma aziendale al fine di identificare quali sono le relazioni tra i trattamenti di dati definiti al punto 2 e le funzioni aziendali. Tale mappa serve anche ad identificare le figure attive della sicurezza (titolare, responsabili, incaricati) previste dalla legge. Il riferimento normativo è il punto 19.2 dell'allegato B del d.lgs 196/2003.

4.2. Mappa delle responsabilità



4.3. Strutture di riferimento

4.3.1. Trattamento di dati da parte dell'Ente

Il Comune di Canale d'Agordo effettua il trattamento di dati personali esclusivamente nell'esercizio delle funzioni previste dall'ordinamento vigente per Comuni della Regione Veneto esplicazione delle proprie funzioni e finalità istituzionali.
La raccolta è limitata al dati strettamente necessari, ai sensi della normativa generale vigente, in particolare dei regolamenti comunali, per l'emissione di tutti gli atti e provvedimenti di competenza dell'ente su domanda, quali autorizzazioni, concessioni, permessi, nullaosta, licenze, pareri visti, e nell'ambito delle procedure per acquisire beni e servizi per le attività generali di competenza dell'Ente, per la gestione del personale, per l'erogazione di servizi obbligatori quali soprattutto i servizi di gestione della rete idrica, della raccolta e smaltimento dei rifiuti, ed altri facoltativi quali l'erogazione dell'energia elettrica la fornitura di locali ad associazioni. Sono trattati dati sensibili e giudiziari laddove ciò sia previsto dall'ordinamento vigente.

La struttura organizzativa dell' ente è la seguente:
Segretario comunale (Responsabile di tutti i Servizi/Uffici)
Servizio/ufficio segreteria
Servizio/ufficio finanziario
Servizio/ufficio tributi
Servizio/ufficio demografico
Servizio/ufficio tecnico
Servizio di Polizia Municipale

4.3.2. Segretario comunale

Il Segretario comunale è il funzionario più elevato in grado del Comune, partecipa alle riunioni del Consiglio e della Giunta e ne redige i relativi verbali apponendovi la propria firma. Nel rispetto delle direttive impartitegli dal Sindaco da cui dipende funzionalmente, sovrintende allo svolgimento delle funzioni dei responsabili dei servizi/uffici e ne coordina l'attività, coordina i funzionari incaricati di funzioni dirigenziali, dirige gli uffici e i servizi dell'ente, cura l'attuazione dei provvedimenti, è responsabile dell'istruttoria delle deliberazioni, provvede per la loro pubblicazione e provvede ai relativi atti esecutivi, non affidati ai responsabili dei servizi. Esercita ogni altra attribuzione affidatagli dalle Leggi, dallo Statuto e dai Regolamenti ed adempie ai compiti affidatigli dal Sindaco e - se da questi richiesto - roga i contratti e gli atti nei quali il Comune è parte contraente.
Nell'organizzazione del Comune di Canale d'Agordo vengono assegnati al Segretario i compiti di provvedere ad attuare gli indirizzi e gli obiettivi stabiliti dagli organi di governo dell' ente, perseguendo livelli ottimali di efficacia ed efficienza secondo le direttive impartite dal Sindaco. Oltre alle competenze proprie del responsabile del servizio nel settore specificatamente assegnato, anche in funzione del fatto che quello di segretario è ruolo sovraordinato nella dotazione organica dell'ente, allo stesso spettano le funzioni di sovrintendenza, di coordinamento generale e dei funzionari incaricati di posizione organizzativa, degli uffici e dei servizi, che risultano necessarie per l'assolvimento dei compiti assegnati. Fatte salve le competenze, l'autonomia e la responsabilità dei singoli incaricati di responsabilità di servizio, le funzioni di coordinamento e direzione del segretario sono assolte con atti di coordinamento e direzione, al fine di conformare l'azione amministrativa agli indirizzi espressi dal Sindaco e dalla Giunta comunale. Svolge attività di consulenza e supporto legale all'attività di tutti i servizi. Sono riservate al Segretario comunale tutte le funzioni espressamente assegnate a tale organo dalle leggi statati, regionali e provinciali, dai regolamenti comunali e dal documento di organizzazione.
Assume alcune funzioni e compiti ai sensi della normativa in materia di sicurezza sul lavoro, fatte salve le competenze in materia di manutenzione straordinaria e ordinaria degli immobili, delle attrezzature di cantiere, della dotazione di dispositivi di protezione individuale del personale operaio.
Al Segretario può venir assegnata, con specifici atti di indirizzo o provvedimenti del Sindaco la responsabilità di uno o più o di tutti i servizi comunali.
Gestisce le polizze assicurative.

4.3.3. Servizio/Ufficio segreteria

Competenze del Servizio/ufficio:
servizi di segreteria generale e di supporto ai restanti servizi/uffici comunali;
produzione, archivi azione, pubblicazione degli atti di Sindaco, Giunta e Consiglio;
Archiviazione di copia dei provvedimenti adottati dai Responsabili dei Servizi e pubblicazione;
procedure concorsuali e assunzione del personale;
formazione ed aggiornamento del personale;
costituzione di forme collaborative per la gestione dei servizi pubblici con altri enti;
coordinamento degli atti deliberativi e delle determinazioni;
attività contrattuale riferita alla fornitura di servizi di assistenza e manutenzione;
attività di sportello.

4.3.4. Servizio/ufficio finanziario

Competenze del Servizio:
gestione del bilancio e programmazione finanziaria
gestione delle risorse di cassa ed investimenti fruttiferi
gestione economico-giuridica e previdenziale del personale
registrazione presenze personale
gestione rendiconti e contabilità convenzioni ed iniziative in
collaborazione con altri enti ed amministrazioni - accertamento delle entrate
procedimenti di acquisto o alienazione di beni immobili;
contributi ad enti ed associazioni
funzioni di responsabile dei tributi
assunzione di mutui per investimenti;
ricovero presso istituti
adempimenti fiscali
rapporti con il tesoriere
gestione economale ed utilizzo immobili comunali
statistiche finanziarie
gestione servizio mensa scolastica infanzia e rette scuolabus

4.3.5. Servizio/Ufficio tributi

Competenze del servizio:
gestione imposte e tasse (in particolare I.C.I., T.O.S.A.P., T.A.R.S.U.)
gestione del sistema informatico (software e hardware) dei servizi comunali
accertamento delle entrate specificate nell' atto di indirizzo
istruttoria contenzioso tributi locali (I.C.I. escluso)
attività preparatoria per determinazione tariffe e aliquote tributi
attività di sportello

4.3.6. Servizio/Ufficio demografico

Competenze del Servizio/ufficio:
servizi di stato civile con delega alle funzioni di Ufficiale di Stato Civile
funzioni anagrafiche con delega
funzioni elettorali con delega
censimento della popolazione ed agricoltura
leva militare
commercio, esercizi pubblici ed altre attività economiche
protocollo, gestione archivi e pubblicazioni
attività di sportello

4.3.7. Servizio/Ufficio tecnico

Competenze del Servizio/ufficio:
rilascio di autorizzazioni e concessioni di attività edilizia privata, nel rispetto delle procedure previste dal vigente Regolamento edilizio comunale;
sorveglianza e controllo dell'attività edilizia privata compresi gli eventuali provvedimenti repressivi;
assistenza e controllo dell'attività edilizia pubblica per quanto riguarda il rispetto delle norme contrattuali, capitolati speciali, acquisizione di pareri ed assolvimento di incombenze riguardanti attività espropriativa;
redazione di perizie, verbali di sopralluogo e quant'altro riferito a lavori da eseguirsi in economia, compresa l'eventuale redazione di computi e direzione lavori e contabilità, qualora affidati con specifico provvedimento od ordine di servizio;
direzione e controllo dell'attività del cantiere comunale, compresa l'ordinazione di materiali per assicurare il funzionamento degli impianti degli edifici comunali e delle opere di urbanizzazione primarie; istruzione di pratiche riferite alla richiesta/variazione di utenze dei servizi comunali e quant'altro possa contenere risvolti di carattere tecnico;
emissione di ordinanze di competenza dell'ufficio per quanto riguarda il suolo pubblico ed i servizi in generale;
attività attinenti i servizi di prevenzione e protezione ai sensi del D.Lgs. 81/2008 e successive modificazioni ed integrazioni, relativamente agli edifici ed impianti ed alla dotazione dei dispositivi di protezione personale;
procedimenti di acquisto o alienazione di beni immobili;
attività di sportello

4.3.8. Servizio/Ufficio di Polizia Municipale

Competenze del servizio:
notifiche atti dell' ente e di terzi
servizi di polizia urbana
servizi di polizia cimiteriale
servizi di polizia metrica e di commercio
servizi di polizia edilizia
servizi di polizia rurale con attività di vigilanza e controllo del patrimonio forestale nell'ambito del censuario comunale, gestione lotti boschivi, assistenza a martellate e misurazioni del legname
assegnazioni di legna e legname uso interno.

5. Analisi dei rischi che incombono sui dati

5.1. Scopo

In questa sezione vengono individuati i principali eventi potenzialmente dannosi per la sicurezza dei dati e vengono valutate le possibili conseguenze e la gravità.
Per ogni evento dannoso viene descritta la contromisura prevista. Il riferimento normativo è il punto 19.3 dell'allegato B del D.Lgs 196/2003.
Per contromisura si intende non solo lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia. Senza procedure di controllo periodico, infatti, nessuna misura può essere considerata completa.

5.2. Elenco dei potenziali eventi dannosi

Per ogni evento è proposto un codice della contromisura, la cui descrizione dettagliata è riportata nelle schede della successiva sezione 4.3. Nel caso in cui la contromisura è relativamente semplice viene indicata direttamente nella relativa colonna senza riferimenti a ulteriori schede.

Evento	Provenienza/Causa	Descrizione	Probabilità che l'evento si verifichi B=Bassa; M=Media; A=Alta	Gravità dei danni stimata B=Bassa M=Media A=Alta	Codice contromisura o descrizione
Furto di credenziali di autenticazione	Comportamenti degli operatori	Incauta custodia delle password da parte degli utenti oppure il responsabile della custodia delle parole chiave non adotta le contromisure necessarie a garantire la segretezza delle credenziali degli utenti	B	A	Nomina di un responsabile della custodia delle parole chiave Formazione agli incaricati sulle proprie responsabilità e sulle norme di "buon comportamento" Obbligo di cambio della password secondo i termini di legge (ogni 6 mesi oppure 3 mesi per dati sensibili/giudiziari)
Carenza di consapevolezza, disattenzione o incuria	Comportamenti degli operatori	Possibile cancellazione o modifica dei dati	B	A	Formazione agli incaricati sul corretto uso e custodia dei trattamenti di dati affidati Sistema di backup (BCK01)
Comportamenti sleali o fraudolenti	Comportamenti degli operatori	Possibile furto e relativa comunicazione o diffusione di dati	B	A	Formazione agli incaricati sulle proprie responsabilità e sulle norme di "buon comportamento", in particolare limitare l'utilizzo di supporti removibili e posta elettronica alle finalità previste dalla mansione.
Errore materiale	Comportamenti degli operatori	Possibile cancellazione o modifica accidentale dei dati	B	A	Formazione agli incaricati sul corretto uso e custodia dei trattamenti di dati affidati Sistema di backup (BCK01)
Azione di virus informatici o di codici malefici	Eventi relativi agli strumenti	Possibile cancellazione, modifica dei dati per aziende di virus, worm e altri programmi dannosi. Possibile diffusione di dati attraverso l'azione di virus che agiscono sulla posta elettronica	M	A	Sistema antivirus (VIR01)

Altre tecniche di sabotaggio	Eventi relativi agli strumenti	Possibile azioni di sabotaggio sfruttando la vulnerabilità degli strumenti o falle di sicurezza causate ad una errata o incompleta configurazione delle apparecchiature	B	M	Nomina di un amministratore di sistema che si occupi della verifica periodica degli aggiornamenti disponibili per il software installato ed eventuali aggiornamenti firmware delle apparecchiature
Accessi esterni non autorizzati	Eventi relativi agli strumenti	Possibile intrusione dalla Rete Internet sfruttando "porte" lasciate aperte inavvertitamente o per telecontrollo/teleassistenza collegamento remoto	M	A	Sistema firewall (FIR01)
Intercettazione di informazioni in rete	Eventi relativi agli strumenti	Possibile intercettazione di dati che transitano sulla rete locale oppure accesso a cartelle di rete non protette	B	A	Server di dominio (SER01)
Accessi non autorizzati a locali/reparti ad accesso ristretto	Eventi relativi al contesto	Possibile accesso non autorizzato ad aree dove è effettuato il trattamento dei dati (principalmente in formato cartaceo)	B	A	Chiusura a chiave dei locali dopo l'orario di lavoro, segnalazione delle aree soggette ad accesso riservato agli incaricati del trattamento, sorveglianza dei locali e degli strumenti da parte degli incaricati al trattamento durante l'orario di lavoro. Sistema antifurto (ANT01).
Asportazione e furto di strumenti contenenti dati	Eventi relativi al contesto	Possibile accesso non autorizzato ad aree dove è effettuato il trattamento dei dati (principalmente in formato cartaceo) e furto delle informazioni	B	A	Chiusura a chiave dei locali dopo l'orario di lavoro, segnalazione delle aree soggette ad accesso riservato agli incaricati del trattamento, sorveglianza dei locali e degli strumenti da parte degli incaricati al trattamento durante l'orario di lavoro. Cassaforte utilizzata per i documenti particolarmente riservati.
Eventi distruttivi, naturali e artificiali, dolosi, accidentali o dovuti ad incuria	Eventi relativi al contesto	Possibile guasto delle apparecchiature (dischi fissi in particolare), rischio incendio, allagamento	M	A	Contromisure antincendio (ANT01)
Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc)	Eventi relativi al contesto	Possibile mancanza di alimentazione elettrica	B	B	Sistema UPS
Errori umani nella gestione della sicurezza fisica	Eventi relativi al contesto	Mancata copia di salvataggio di sicurezza dei dati e negligenza nella custodia delle copie di sicurezza	B	A	Nomina di un responsabile della copie di sicurezza dei dati

5.3. Schede descrittive delle contromisure adottate

Codicecontromisura	BCK01
Descrizione breve	Sistema di backup
Trattamenti interessati e/o ambiti di applicazione	
Rischio da contrastare	Cancellazione di dati per azione accidentale da parte degli operatori o guasto delle apparecchiature
Descrizione (modelli, marche, tecnologia, etc)	Windows 2003 Server
Eventuali banche dati interessate	tutte
Misura già in essere ? (SI/NO)	[X] Si [ ] No
Tipologia della misura di sicurezza	[X] Preventiva [ ] Di contrasto [ ] Di contenimento degli effetti [ ] Altro:
Misura da adottare entro il	
Responsabilità del controllo	personale incaricato
Periodicità del controllo	Giornaliera
Note	
Scheda contromisura compilata da:	

Codicecontromisura	VIR01
Descrizione breve	Sistema antivirus
Trattamenti interessati e/o ambiti di applicazione	Tutti
Rischio da contrastare	Azione di programmi dannosi: Virus, Worm, etc
Descrizione (modelli, marche, tecnologia, etc)	AGV antivirus businnes edition
Eventuali banche dati interessate	
Misura già in essere ? (SI/NO)	[X] Si [ ] No
Tipologia della misura di sicurezza	[ ] Preventiva [X] Di contrasto [X] Di contenimento degli effetti [ ] Altro:
Misura da adottare entro il	
Responsabilità del controllo	personale incaricato
Periodicità del controllo	Giornaliera
Note	
Scheda contromisura compilata da:	

Codicecontromisura	FIR01
Descrizione breve	Sistema firewall
Trattamenti interessati e/o ambiti di applicazione	Tutti
Rischio da contrastare	Blocco di accessi non autorizzati dalla rete internet

Descrizione (modelli, marche, tecnologia, etc)	Sistema firewall
Eventuali banche dati interessate	Tutte
Misura già in essere ? (SI/NO)	[X] Si [ ] No
Tipologia della misura di sicurezza	[ ] Preventiva [X] Di contrasto [X] Di contenimento degli effetti [ ] Altro:
Misura da adottare entro il	
Responsabilità del controllo	personale incaricato
Periodicità del controllo	
Note	
Scheda contromisura compilata da:	

Codicecontromisura	SER01
Descrizione breve	Sistema server Windows
Trattamenti interessati e/o ambiti di applicazione	
Rischio da contrastare	Accesso ad informazioni di rete non protette
Descrizione (modelli, marche, tecnologia, etc)	Server Windows 2003
Eventuali banche dati interessate	
Misura già in essere ? (SI/NO)	[X] Si [ ] No
Tipologia della misura di sicurezza	[ ] Preventiva [X] Di contrasto [X] Di contenimento degli effetti [ ] Altro:
Misura da adottare entro il	
Responsabilità del controllo	personale incaricato
Periodicità del controllo	
Note	
Scheda contromisura compilata da:	

Codicecontromisura	UPS01
Descrizione breve	Sistema di alimentazione supplementare UPS
Trattamenti interessati e/o ambiti di applicazione	
Rischio da contrastare	Mancanza di alimentazione di rete
Descrizione (modelli, marche, tecnologia, etc)	Gruppo di continuità per server
Eventuali banche dati interessate	
Misura già in essere ? (SI/NO)	[X] Si [ ] No
Tipologia della misura di sicurezza	[ ] Preventiva [X] Di contrasto [ ] Di contenimento degli effetti [ ] Altro:
Misura da adottare entro il	
Responsabilità del	personale incaricato

controllo	
Periodicità del controllo	trimestrale
Note	

Codicecontromisura	ANT01
Descrizione breve	Contromisure antincendio
Trattamenti interessati e/o ambiti di applicazione	
Rischio da contrastare	Incendio archivi informatici e cartacei
Descrizione (modelli, marche, tecnologia, etc)	Estintore posizionato in prossimità degli archivi
Eventuali banche dati interessate	
Misura già in essere ? (SI/NO)	[X] Si [ ] No
Tipologia della misura di sicurezza	[ ] Preventiva [X] Di contrasto [ ] Di contenimento degli effetti [ ] Altro:
Misura da adottare entro il	
Responsabilità del controllo	Soggetti esterni incaricati
Periodicità del controllo	Trimestrale
Note	

5.4. previsione per eventuali adeguamenti tecnici o miglioramenti tecnico/organizzativi

Considerata la rapida evoluzione tecnologica e la relazione tra vulnerabilità degli strumenti elettronici e la loro obsolescenza, il Titolare del Trattamento, dopo aver valutato attentamente l'attuale situazione tecnica, considerato il raggiungimento degli standard minimi richiesti dalle misure minime di sicurezza all'allegato B del D.Lgs 196/2003, si riserva comunque nel breve-medio periodo di intervenire sul parco macchine pc, utilizzando la seguente linea guida, per imporre miglioramenti generali degli standard tecnico-qualitativi e quindi aumentare il grado di sicurezza:

corso di formazione di base sulla rete e sulla privacy
chiusura in un armadio con chiave del router e degli switch di rete

Dal punto di vista organizzativo il Titolare dichiara che nel corso dell'anno 2011 saranno progressivamente rivisti gli accessi ai locali, verificando quali persone sono dotate di chiave per accedere ai locali, limitando l'accesso ai locali qualora non venisse giustificata la presenza della persona in funzione del trattamento di dati da effettuare nel locale alla quale la persona accede.
Il Titolare dichiara inoltre che con cadenza annuale saranno verificato il posizionamento e la sicurezza degli archivi cartacei, con particolare attenzione ai dati sensibili/giudiziari che dovranno essere archiviati separatamente rispetto ai dati personali. In fase di verifica inoltre si controllerà l'eventuale necessità di limitare l'accesso al pubblico per particolari aree o zone negli uffici o nell'edificio comunale.

6. Criteri e modalità di ripristino della disponibilità dei dati

6.1. Scopo

In questa sezione sono descritti i criteri e le procedure adottare per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati.
L'importanza di queste attività deriva direttamente dalla eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che quando sono necessarie le copie dei dati siano disponibili e le procedure siano efficaci.
Il riferimento normativo è la regola 19.5 dell'allegato B del d.lgs 196/2003.

Sistema o set di backup	Cassetta
Ambito del backup	Tutti i file relativi a tutti i trattamenti
Ciclicità del backup	5 cassette a rotazione giornaliera
Struttura operativa incaricata del salvataggio	Tributi
Ubicazione delle copie di sicurezza	Cassaforte, situata nel locale ragioneria
Sono state effettuate le prove di ripristino	[X] Si [ ] No
Modalità di ripristino dei dati	In caso di necessità di ripristino dei dati il personale addetto si occupa della manutenzione del backup, attualmente incarico affidato al personale dell'ufficio Tributi. Il personale autorizzato a gestire il backup è a conoscenza della procedura.

7. Pianificazione degli interventi formativi previsti

7.1. Scopo

In questa sezione sono riportate le informazioni necessarie per disporre di un quadro sintetico dell'impegno formativo che si prevede di sostenere in attuazione della normativa.
Il riferimento normativo è il punto 19.6 dell'allegato B del D.Lgs 196/2003.

7.2. Planning e descrizione degli interventi formativi a cura del titolare

Identificativo del corso di formazione	Docente o ente incaricato per la formazione	Numero di incaricati interessati	Tipologia di incaricati	Calendario
Generale	Esterno	8	Impiegati	2011

7.3. Disposizioni scritte

Il titolare dichiara inoltre che sono state fornite agli incaricati disposizioni scritte in merito alla corretta applicazione delle disposizioni presenti nell'allegato B (misure minime di sicurezza) del d.lgs 106/2003.

8. Trattamenti affidati all'esterno

8.1. Scopo

Obiettivo di questa sezione è redigere un quadro sintetico delle attività trasferite a terzi che comportano il trattamento di dati personali con l'indicazione sintetica del quadro contrattuale in cui tale trasferimento si inserisce, in riferimento alla protezione dei dati personali. Il riferimento normativo è il punto 19.7 dell'allegato B del d.lgs. 2003.

8.2. Attività in out-sourcing e soggetti esterni

Attività in outsourcing	Tipologia di dati personali, sensibili o giudiziari interessati	Soggetto Esterno
Servizi di gestione ed elaborazione paghe del personale dipendente con gestione complessive contributiva e fiscale, cud, 770 etc.	Personali sensibili	Comunità Montana Agordina
Gestione diritto pubbliche affissioni e imposta comunale sulla pubblicità	Personali	DUOMO GPA srl, Viale Sarca, 195 Milano
Fornitura e assistenza e tele assistenza software ASCOT WEB	Personali	INSIEL S.p.A., via San Francesco d'Assisi, 43 Trieste
Servizio di aggiornamento inventario patrimonio mobiliare ed immobiliare (dei beni comunali)	Personali	Doc Service SRL Via Degasperi, 77 TRENTO
Servizio 626 RSPP, MEDICO COMPETENTE DEL LAVORO	Personali sensibili	dottor Domenico Grazioli, Sass de Mura – Soranzen Cesiomaggiore (BL) -FINO AL 2010- In fase di nuova individuazione
Servizio di tesoreria	Personali	Cassa Rurale Val di Fassa e Agordino, Piaz de Stegrava, 1 – Moena (TN)
Servizio di revisore contabile	Personali sensibili	Dott. Patrick Da Pos, Piazza Libertà, 6 Agordo (BL)
Servizio di incasso e gestione contabile I.C.I.	Personali sensibili	Equitalia Nomos spa, Via dell'Arcivescovado, 8 Torino
Gestione servizio controllo e contenzioso I.C.I.	Personali sensibili	Comunità Montana Agordina
Gestione del servizio raccolta rifiuti	Personali sensibili	Comunità Montana Agordina

9. Cifratura dei dati o separazione dei dati identificativi

9.1. Contenuti

Il punto 19.8 dell'allegato B prevedere una sezione del DPS a cura degli organismi sanitari e gli esercenti le professioni sanitarie che dichiari le modalità di protezione adottare per i dati per cui è richiesta la cifratura la separazione fra dati identificati e dati personali.
Per la natura dei dati dichiarati dal titolare del trattamento dei dati e le finalità del trattamento nonché l'attività svolta dalla struttura non si ritiene necessaria l'applicazione di forme di cifratura o separazione dei dati.

10. Documentazione aggiuntiva

10.1. Documentazione

Si è provveduto a predisporre le lettere di nomina alle varie figure incaricate dell'attuazione del presente documento programmatico sulla sicurezza.
Si dichiara inoltre di aver dato disposizione affinché tale documentazione sia aggiornata costantemente con l'evoluzione del personale e delle collaborazione esterne.

11. Dichiarazioni finali

Il titolare del trattamento dei dati dichiara che le informazioni contenute nel presente Documento Programmatico sulla Sicurezza dei dati e negli allegati corrispondono al vero e che le informazioni rilevate ai fini della definizione dell'elenco del trattamento dei dati, dei profili degli incaricati e dei responsabili e tutte le informazioni sono state verificate.
Dichiara inoltre di essere a conoscenza che :
il Titolare del trattamento è 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.
Il Titolare del trattamento deve assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.
Il Titolare del trattamento, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più Responsabili della sicurezza dei dati che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA. Qualora il Titolare del trattamento ritenga di non nominare alcun Responsabile della sicurezza dei dati, ne assumerà tutte le responsabilità e funzioni.

Canale d'Agordo, 30/03/2011

Comune di Canale d'Agordo
Segretario Comunale Pierfilippo Fattori
Sindaco pro-tempore Rinaldo De Rocco