Comune di Carovigno

Provincia di Brindisi

Codice in materia di protezione dei dati personali
Documento programmatico sulla sicurezza

XV Censimento Generale della Popolazione
e delle Abitazioni

Ottobre 2011

Redatto da Ing. Pierluigi Zurlo

Ufficio Sistemi Informativi, Elaborazione dati
Comune di Carovigno - Via Verdi 1, 72012 Carovigno (BR)
www.comune.carovigno.br.it
Centralino: 0831 997 111 - Fax: 0831 99 20 20
E-mail: Pierluigi.zurlo@comune.carovigno.br.it
PEC: ced.comune.carovigno@pec.rupar.pulgia.it

INDICE

1. Introduzione normativa

Nel 2003 è stato completato l'iter normativo di integrazione e razionalizzazione della disciplina in materia di protezione dei dati personali. Infatti con il DLgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), per la prima volta nel panorama internazionale viene riunita in un unico corpo normativo, di rango legislativo, una materia, quella della protezione dei dati, la cui disciplina si era formata nel tempo con vari interventi integrativi e modificativi della L. 31 dicembre 1996, n. 675.
La nuova disciplina, però, non si limita a raccogliere in un quadro sistematico le precedenti leggi a formazione labirintica, ma presenta anche interventi più incisivi di carattere strutturale e di principi, ampliando inoltre la tutela riconosciuta a livello comunitario, contemplando non solo le persone fisiche ma anche le persone giuridiche.
L'innovazione sul piano dei principi si coglie fin dal primo articolo del Codice, che riproduce il primo comma dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea "Chiunque ha diritto alla protezione dei dati personali che lo riguardano".

Il legislatore ha voluto ulteriormente ribadire la sua volontà di considerare la protezione dei dati come un diritto fondamentale, nominandola esplicitamente nell'articolo 2 del Codice che recita:

> comma 1 - Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali 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.
>
> comma 2 - Il trattamento dei dati personali e' disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 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 dei titolari del trattamento."

Oggetto della tutela non sono più le banche dati, che diventano i contenitori dei dati personali, ma oggetto della tutela sono i dati personali stessi, nella consapevolezza che il legislatore fa risaltare che un cattivo uso o addirittura un abuso o un uso illegittimo di dati personali che riguardino persone fisiche o persone giuridiche può compromettere diritti e libertà fondamentali delle persone.

E' in questo quadro che si inseriscono le previsioni normative previste nel TITOLO V del codice in materia di sicurezza dei dati e dei sistemi e nel relativo Allegato B al Codice "Disciplinare tecnico in materia di misure minime di sicurezza". In particolare:

- L'art. 31 "Obblighi di sicurezza" stabilisce che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, in modo a ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi 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'art. 33 "Misure minime" stabilisce che, nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque

tenuti ad assicurare un livello minimo di protezione dei dati personali attraverso l'adozione di misure minime di sicurezza, intendendosi per tali il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

- L'art. 34 "Trattamenti con strumenti elettronici" del medesimo Decreto, stabilisce che il trattamento di dati personali effettuato con strumenti elettronici – intendendosi per tali gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento - è consentito solo se sono adottate,nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
  a) autenticazione informatica, intendendosi per tale l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
  b) adozione di procedure di gestione delle credenziali di autenticazione, intendendosi per tali i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
  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.

- L'art. 35 "Trattamenti senza l'ausilio di strumenti elettronici" del medesimo Decreto, stabilisce che il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
  a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
  b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
  c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

- Il punto n. 19 dell'allegato " B - Disciplinare tecnico in materia di misure minime di sicurezza" prevede che il Titolare di trattamenti di dati Sensibili o Giudiziari entro il 31 marzo di ogni anno rediga e predisponga un apposito DOCUMENTO PROGRAMMATICO SULLA SICUREZZA", nel quale devono essere indicati:
  - l'elenco di trattamenti di dati personali;
  - la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
  - l'analisi dei rischi che incombono sui dati;
  - le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

- la descrizione dei criteri e delle modalità per il ripristino delle disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi per gli Incaricati del trattamento, per renderli edotti sui rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal Titolare;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza nel caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del Titolare.

Elenco dei trattamenti *Informazioni di base* *(regola 19.1 allegato B al Codice)*

Definizioni (da art. 4 Codice)

- «trattamento», qualunque operazione o complesso di operazioni, …, concernenti la raccolta, la registrazione, …, l'elaborazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

  nell'ambito del 15° Censimento generale della popolazione e delle abitazioni:

  ogni operazione , richiamata dalla normativa, riguardante dati personali, svolta dall'Istat, dagli organi di censimento e dagli altri soggetti coinvolti nel censimento.

- «dato personale», qualunque informazione relativa a persona fisica, giuridica, ente od associazione, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

  nell'ambito del 15° Censimento generale della popolazione e delle abitazioni:

  qualunque informazione riferita agli individui che sono oggetto di rilevazione nell'ambito del Censimento.

- «dati identificativi», i dati personali che permettono l'identificazione diretta dell'interessato.

- «dati anonimi», I dati che in origine, o a seguito di trattamento, non possono essere associati ad un interessato identificato o identificabile.

- «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;

- «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.

- «banca di dati», qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- «interessato», la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Nell'ambito del 15° Censimento generale della popolazione e delle abitazioni:

sono *interessati* tutti gli individui che sono oggetto di rilevazione nell'ambito del Censimento e gli operatori coinvolti nelle attività censuarie (i cui dati personali sono trattati per esigenze organizzative).

2. Strutture preposte al trattamento dei dati *(regola 19.2 allegato B al Codice)*

2.1 Segreto statistico e protezione dei dati personali

L'Istat è tenuto per legge a rispettare il segreto statistico sui dati raccolti in occasione delle proprie rilevazioni (art. 9 del d.lgs. n. 322/89 istitutivo del Sistema statistico nazionale).

Tali dati, pertanto, sono utilizzati esclusivamente a fini statistici e non possono essere comunicati ad alcun soggetto - pubblico o privato - estraneo al Sistema statistico nazionale, né possono essere diffusi, se non in forma aggregata e in modo tale che non sia possibile identificare la persona a cui le informazioni si riferiscono.

Il rispetto del segreto statistico si inserisce nella più ampia tutela dei dati personali prevista dal Codice in materia di protezione dei dati personali (d.lgs. n. 196/03) e, in particolare, dall'allegato A3 denominato "Codice di deontologia per il trattamento di dati personali a scopi statistici in ambito Sistan".

Anche la statistica ufficiale, deve, pertanto, tutelare i diritti, le libertà fondamentali e la dignità dei rispondenti, con particolare riguardo al diritto, alla riservatezza e all'identità personale.

Per rendere effettiva la tutela del segreto statistico e la protezione dei dati personali l'Istat appronta adeguate misure organizzative, logistiche, informatiche, metodologiche e statistiche, secondo gli standard definiti in sede internazionale.

2.2 Diritti degli interessati

Titolare del trattamento dei dati personali è l'Istat Via Cesare Balbo, 16 – 00184 Roma; responsabili del trattamento sono i Direttori centrali dell'Istituto, ai quali è possibile rivolgersi per l'esercizio dei diritti dell'interessato; incaricati sono tutti i dipendenti che svolgono operazioni di trattamento dei dati.

I soggetti esterni che collaborano con l'Istat all'esecuzione delle indagini sono anch'essi designati responsabili o incaricati del trattamento.

2.3 Figure partecipanti al trattamento dei dati

Titolare del trattamento

- **ISTAT** Via Cesare Balbo, 16 – 00184 Roma

Responsabili del trattamento

- Direttore ISTAT Direzione Centrale Censimenti Generali
- Responsabili degli Uffici di censimento

Incaricati del trattamento

- Personale degli Uffici di censimento
- Coordinatori comunali
- Rilevatori
- Ogni altro operatore coinvolto nelle attività censuarie (componenti CTR, ..)

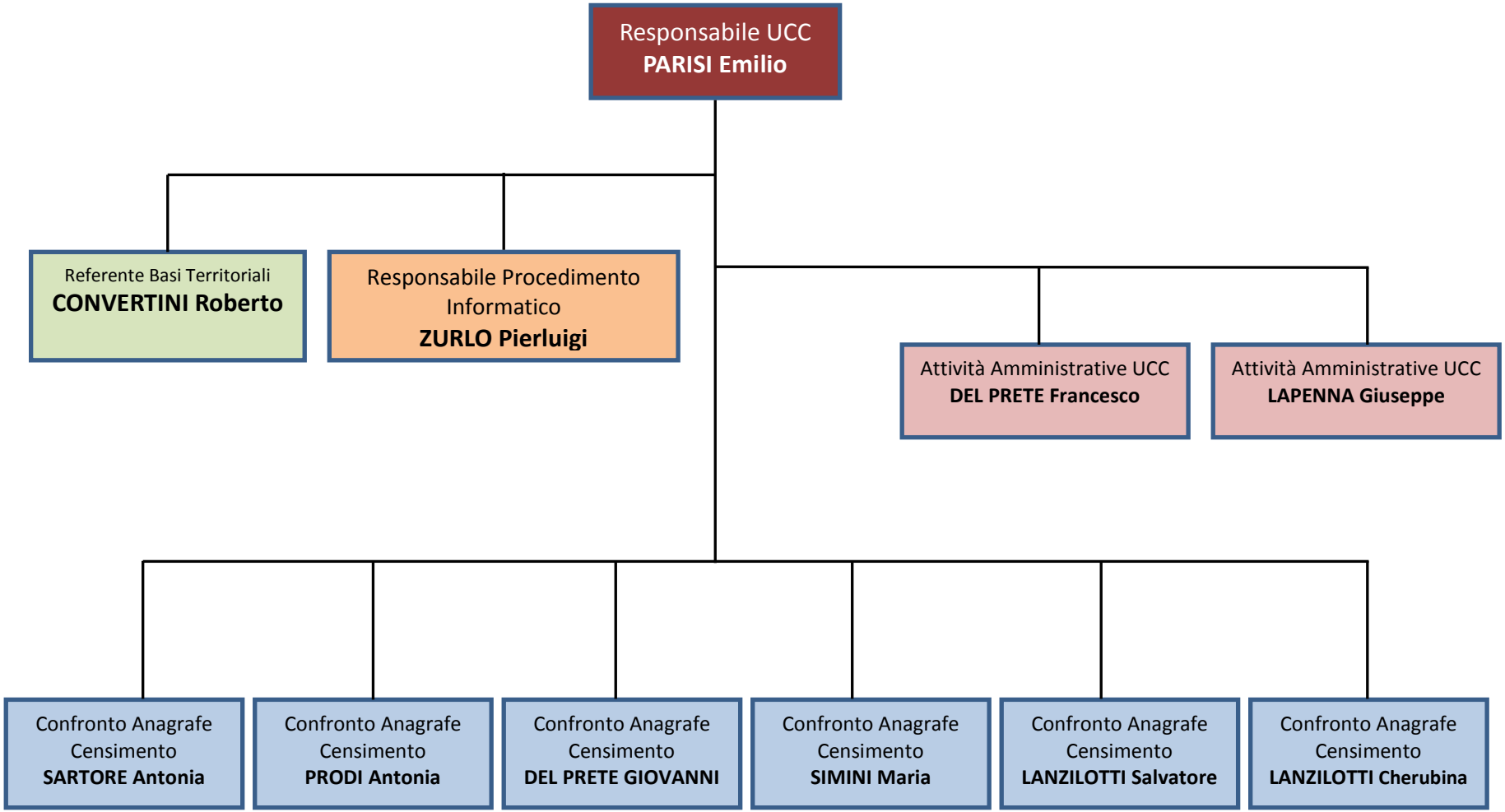
Interessati

- Tutti gli individui oggetto della rilevazione

Struttura Organizzativa al e relativo funzionigramma dell'Ufficio Comunale di Censimento (costituito in forma autonoma) approvati con DGC n. 87 del 01/04/2011

	Cognome	Nome	Ufficio di appartenenza	Profilo professionale	Compiti di massima assegnati
1	PARISI	Emilio	Sviluppo del Territorio	Responsabile del Servizio	Responsabile UCC
2	ZURLO	Pierluigi	Sistemi Informativi	Collaboratore Professionale	Responsabile Procedimento Informatico
3	CONVERTINI	Roberto	Urbanistica	Istruttore Direttivo Tecnico	Referente Basi Territoriali
4	DEL PRETE	Francesco	Demografico	Collaboratore Informatico	Attività Amministrative UCC
5	LAPENNA	Giuseppe	Patrimonio	Istruttore Tecnico	Attività Amministrative UCC
6	DEL PRETE	Giovanni	Tecnico	Autista di fatto Collaboratore Professionale	Confronto Anagrafe Censimento
7	SARTORE	Antonia	Demografico	Collaboratore Informatico	Confronto Anagrafe Censimento
8	PRODI	Antonia	Demografico	Collaboratore Informatico	Confronto Anagrafe Censimento
9	SIMINI	Maria	Commercio	Collaboratore Informatico	Confronto Anagrafe Censimento
10	LANZILOTTI	Salvatore	Protocollo	Istruttore Amministrativo	Confronto Anagrafe Censimento
11	LANZILOTTI	Cherubina	Polizia Municipale	Collaboratore Informatico	Confronto Anagrafe Censimento

Funzionigramma



Utenze attive in SGR – Sistema di Gestione della Rilevazione

Identificativo Operatore	Cognome	Nome	Data di Nascita	Profilo Applicativo	Coordinatore
0740020001	Parisi	Emilio	04-11-1947	Responsabile UCC	
0740020002	Sisto	Giovanna	07-03-1973	CoC	
0740020003	Antelmi	Giovanni	03-12-1961	CoC	
0740020004	Cicoria	Andreina	05-10-1967	CoC	
0740020005	Zurlo	Pierluigi	31-12-1981	CoR	
0740020006	Melone	Giuseppina	04-12-1981	Ril. media operat.	Sisto Giovanna
0740020007	Tateo	Maria Carmela	29-07-1983	Ril. media operat.	Antelmi Giovanni
0740020008	Carlucci	Francesca	16-02-1985	Ril. media operat.	Sisto Giovanna
0740020009	Lanzilotti	Pasquale	30-11-1984	Ril. media operat.	Antelmi Giovanni
0740020010	Natola	Cosima	26-10-1982	Ril. media operat.	Cicoria Andreina
0740020011	Pantaleo	Luca	18-06-1980	Ril. media operat.	Cicoria Andreina
0740020012	Saponaro	Teresa	16-10-1985	Ril. media operat.	Cicoria Andreina
0740020013	Caliolo	Anna	03-07-1985	Ril. media operat.	Sisto Giovanna
0740020014	Iaia	Carmela	28-05-1976	Ril. media operat.	Sisto Giovanna
0740020015	Tamborrino	Cristiano	03-11-1981	Ril. media operat.	Cicoria Andreina
0740020016	Salonna	Marco Tommaso	13-08-1983	Ril. media operat.	Cicoria Andreina
0740020017	Di Dio	Giordana	07-11-1976	Ril. media operat.	Sisto Giovanna
0740020018	Greco	Domenico	21-11-1988	Ril. media operat.	Sisto Giovanna
0740020019	Tateo	Paolo Giuseppe	25-07-1987	Ril. media operat.	Antelmi Giovanni
0740020020	Caliolo	Maddalena	20-11-1986	Ril. media operat.	Antelmi Giovanni
0740020021	Caroli	Laura	15-07-1984	Ril. media operat.	Antelmi Giovanni
0740020022	Cavaliere	Laura	04-01-1976	Ril. media operat.	Antelmi Giovanni
0740020023	Fusco	Maria Carmela	20-03-1979	Ril. media operat.	Sisto Giovanna
0740020024	Lanzilotti	Sara	14-07-1983	Ril. media operat.	Cicoria Andreina
0740020025	Marinò	Francesca	16-03-1976	Ril. media operat.	Cicoria Andreina
0740020026	Monna	Nicoletta	25-08-1971	Ril. media operat.	Antelmi Giovanni
0740020027	Valente	Rosaria	20-07-1979	Ril. media operat.	Antelmi Giovanni
0740020028	Favia	Francesca	04-01-1978	Ril. media operat.	Antelmi Giovanni
0740020029	Del Prete	Mariangela	16-08-1983	Ril. media operat.	Sisto Giovanna
0740020030	Suma	Rosa	11-09-1973	Ril. media operat.	Cicoria Andreina
0740020031	Lanzilotti	Luigi	23-11-1978	Ril. media operat.	Sisto Giovanna
0740020032	Prima	Rossana Maria	23-05-1973	Ril. media operat.	Sisto Giovanna
0740020033	Buongiorno	Lucia Piera	28-06-1974	Ril. media operat.	Antelmi Giovanni
0740020034	Brandi	Gennaro	14-10-1951	Ril. media operat.	Cicoria Andreina

Nota*: elenco soggetto a modifiche dovute a rinunce e/o successivi subentri.*

Elenco degli eventi che possono generare danni

Eventi che impattano sulla sicurezza dovuti a:

- comportamento operatori (da EA001 a EA004)
- eventi relativi agli strumenti (da EB001 a EB006)
- eventi relativi al contesto (da EC001 a EC005)

Evento			Descrizione evento e Impatto sulla sicurezza
Comportamento operatori	E-A001	Sottrazione di credenziali di autenticazione	**Descrizione:** le credenziali (userID/Password) possono essere sottratte al legittimo possessore con vari metodi, anche grazie alla negligenza nella conservazione da parte del possessore stesso.
			Impatto: altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto e per tutto al soggetto possessore delle stesse. Il sistema di protezione non può, in principio, sapere dell'occorrenza di tale furto.
	E-A002	Errore materiale	**Descrizione:** a causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli addetti al trattamento possono compiere operazioni errate o specificare dati errati.
			Impatto: nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati.
	E-A003	Comportamenti illegali conseguenti a minacce su operatori	**Descrizione:** in conseguenza di pressioni di vario tipo (es. minacce, ricatti, pressioni psicologiche) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata all'evento.
			Impatto: nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
	E-A004	Comportamenti sleali e/o fraudolenti	**Descrizione:** con comportamento consapevole, derivate potenzialmente da vari fattori, gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento.
			Impatto: nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
	E-A005	Abuso delle funzioni di Amministratore di Sistema	**Descrizione:** con comportamento consapevole, derivate potenzialmente da vari fattori, gli incaricati di funzione di Amministratore di Sistema possono compiere operazioni illecite anche su ampie parti del sistema informatico.
			Impatto: nei casi più gravi si può ottenere la distruzione di tutto o parte del patrimonio di dati informatici dell'Ente. In molti casi anche il semplice accesso per fini non consentiti a dati personali.

Eventi relativi agli strumenti	E-B001	Virus informatici	**Descrizione:** sul sistema su cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può venirsi ad installare o essere semplicemente eseguito del software spurio del tipo "virus" informatico.
			Impatto: nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
	E-B002	Spamming	**Descrizione:** il sistema di posta elettronica utilizzato dagli incaricati del trattamento dei dati potrebbe essere obiettivo di invii di posta spuria (spam) generata anche con strumenti automatizzati. Tali messaggi possono contenere false notizie.
			Impatto: gli incaricati del trattamento possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non regolari.
	E-B003	Accesso da stazioni non autorizzate	**Descrizione:** soggetti in possesso di credenziali di accesso al sistema, o intenzionati a sferrare un attacco informatico ad uno dei sistemi HW/SW, da cui e possibile intervenite su una banca dato obiettivo, possono accedere al sistema da una postazione non utilizzata in condizioni normali di operatività.
			Impatto: nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
	E-B004	Intercettazione di informazioni transitanti sulla rete	**Descrizione:** soggetti malintenzionati possono catturare, mediante vari sistemi fisici (Snooping, Spoofing), parte delle informazioni che transitano sulla rete informatica dell'Ente. Ciò può avvenire in un qualunque punto interessato tra il sistema utilizzato e il sistema HW/SW degli incaricati.
			Impatto: Nei casi più gravi, mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione di dati da parte dei malintenzionati.
	E-B005	Malfunzionamento apparecchiature	**Descrizione:** I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono avere malfunzionamenti da cui possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati.
	E-B006	Degrado apparecchiature	**Descrizione:** I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono essere soggetti a degrado naturale conseguente all'uso o al solo funzionamento. Da ciò possono derivare azioni reali sui dati parzialmente o totalmente diverse da quelle che si volevano operare.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati.

Eventi relativi al contesto	E-C001	Accesso non autorizzato a locali da cui si può accedere ai dati	**Descrizione:** Un soggetto autorizzato allo scopo, può comunque accedere fisicamente ai locali dai quali è accessibile e manipolabile la banca dati interessata all'evento.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si può ottenere un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
	E-C002	Sottrazione di strumenti contenenti dati e/o programmi	**Descrizione:** I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono venire sottratti illecitamente da parte di altri soggetti non aventi diritto di accedere a tale banca dati.
			Impatto: L'evento comporta la sottrazione, in modo illecito, di dati.
	E-C003	Eventi distruttivi naturali/artificiali accidentali o volontari	**Descrizione:** I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono immagazzinati i dati relativi alla banca dati interessata all'evento, possono essere interessati da eventi distruttivi di origine sia fortuita che dolosa.
			Impatto: Dall'evento può derivare la distruzione totale o parziale della banca dati.
	E-C004	Guasto ai sistemi complementari	**Descrizione:** I sistemi ausiliari necessari al corretto funzionamento degli apparati HW/SW con i quali viene trattata, o che contiene la banca dati interessata all'evento, possono avere malfunzionamenti in conseguenza di varie cause.
			Impatto: Dall'evento può derivare la distruzione totale o parziale della banca dati.
	E-C005	Accesso non autorizzato alla sala Server del Comune	**Descrizione:** Le apparecchiature della sala Server sono state alloggiate in un locale dedicato climatizzato all'interno della sede municipale.
			Impatto: L'accesso alla sala Server può permettere la sottrazione di qualunque banca dati informatica residente su tali macchine.

5. Contromisure per contrastare gli eventi dannosi

Descrizione dei contenuti della tabella:

- Misure Fisiche
- Misure Logiche
- Misure Organizzative

ID Misura	M-001	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Protezione con serratura			
Descrizione estesa					
L'accessibilità agli spazi interessati alla misura è assoggettata alla utilizzazione di una apposita chiave disponibile solo per i soggetti appositamente autorizzati. Archivio cartaceo temporaneo: accesso consentito al Responsabile UCC ed ai suoi collaboratori amministrativi. CRC (Centro di Raccolta Comunale): accesso consentito al Responsabile UCC, ai suoi collaboratori amministrativi. Sala Server: accesso consentito al solo Amministratore di Sistema.					
Modalità controllo adozione		Verifica in campo		Periodicità controllo adozione	giornaliera
Tipologia Misura		Fisica		Data ultimo aggiornamento	09/10/2011

ID Misura	M-002	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Armadi a pareti ignifughe			
Descrizione estesa					
Per la protezione da danni derivanti da incendi viene utilizzato un tipo di armadio di contenimento con pareti in grado di resistere al fuoco ed alle alte temperature per un tempo sufficiente a porre in sicurezza i contenuti dello stesso prima del loro deterioramento.					
Modalità controllo adozione		Verifica in campo		Periodicità controllo adozione	giornaliera
Tipologia Misura		Fisica		Data ultimo aggiornamento	09/10/2011

ID Misura	M-003	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Estintori			
Descrizione estesa					
I locali/vani sono dotati di appositi estintori da utilizzarsi per l'estinzione delle fiamme in caso di incendio.					
Modalità controllo adozione		Verifica in campo		Periodicità controllo adozione	semestrale
Tipologia Misura		Fisica		Data ultimo aggiornamento	09/10/2011

ID Misura	M-004	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Password condivisa di accesso alla stazione informatica (CRC)			
Descrizione estesa					
L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso.					
Modalità controllo adozione		Intervista agli incaricati	Periodicità controllo adozione		semestrale
Tipologia Misura		Fisica	Data ultimo aggiornamento		09/10/2011

ID Misura	M-005	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Password personale di accesso ai calcolatori			
Descrizione estesa					
L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto dalla sola persona a cui è stato affidato da parte dell'Amministratore del sistema.					
Modalità controllo adozione		Intervista agli incaricati	Periodicità controllo adozione		semestrale
Tipologia Misura		Fisica	Data ultimo aggiornamento		09/10/2011

ID Misura	M-006	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Firewall			
Descrizione estesa					
Il traffico di rete generato nell'accesso alla risorsa informatica in questione è controllato da un sistema firewall in grado di individuare, tracciare e bloccare i tentativi di attacco già noti. Le regole di controllo sono aggiornate con regolarità dal fornitore dell'apparato. I file di tracciature di tali tentativi sono controllati dagli amministratori del sistema con regolarità.					
Modalità controllo adozione		Prove di accesso/blocco	Periodicità controllo adozione		semestrale
Tipologia Misura		Logica	Data ultimo aggiornamento		09/10/2011

ID Misura	M-007	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Ingresso sorvegliato nell'orario d'ufficio			
Descrizione estesa					
I locali interessati alla misura sono sorvegliati (nella misura di essere considerati al sicuro) durante le ore d'ufficio poiché i suddetti locali sono adiacenti ad uffici del personale dipendente.					
Modalità controllo adozione		Verifiche in campo	Periodicità controllo adozione		semestrale
Tipologia Misura		fisica	Data ultimo aggiornamento		09/10/2011

ID Misura	M-008	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Informazione/formazione specifica sul rischio			
Descrizione estesa					
Gli incaricati del trattamento sulla banca oggetto della misura sono stati resi edotti, in modo specifico e puntuale, degli eventi dannosi relativi a quella banca dati e sulle misure adottate per contrastare il rischio derivante. Sono state poi date istruzioni operative dettagliate sul come rendere operative le misure di contrasto del rischio.					
Modalità controllo adozione		Interviste ad incaricati	Periodicità controllo adozione		semestrale
Tipologia Misura		Organizzativa	Data ultimo aggiornamento		09/10/2011

ID Misura	M-009	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Antivirus			
Descrizione estesa					
Sui Sistemi interessati al trattamento dei dati in questione sono stati installati opportuni software di protezione dai virus informatici. Tali software sono costantemente aggiornati, in modo automatico, con frequenza almeno giornaliera. In certe situazioni il sistema provvede ad aggiornamenti più frequenti.					
Modalità controllo adozione		Interviste ad incaricati	Periodicità controllo adozione		semestrale
Tipologia Misura		Organizzativa	Data ultimo aggiornamento		09/10/2011

ID Misura	M-010	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Manutenzione Correttiva			
Descrizione estesa					
Sulle apparecchiature HW interessate alla misura sono stati attivati contratti di manutenzione correttiva esterni ricorrendo alle ditte fornitrici degli stessi o a ditte specializzate.					
Modalità controllo adozione		Verifiche amministrative	Periodicità controllo adozione		semestrale
Tipologia Misura		Organizzativa	Data ultimo aggiornamento		09/10/2011

ID Misura	M-011	Compilata da	Ing. Pierluigi Zurlo	Data Creazione	06/10/2011
Descrizione sintetica		Manutenzione Correttiva			
Descrizione estesa					
Le credenziali di accesso, quali password o certificati digitali, vengono rinnovate con una frequenza idonea a garantire la riduzione del rischio d'accesso e d'utilizzo delle banche dati, da parte di soggetti non autorizzati che abbino sottratto o generato, con opportune procedure di password-cracking, le stesse.					
Modalità controllo adozione		Intervista interessati	Periodicità controllo adozione		semestrale
Tipologia Misura		Organizzativa	Data ultimo aggiornamento		09/10/2011