COMUNE
di
CASTILENTI
Provincia di Teramo

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

per la

PROTEZIONE DEI DATI PERSONALI
IN MATERIA DI "MISURE MINIME" DI SICUREZZA

(ai sensi degli artt. 31-36 del D.Lgs. n. 196/2003 e del relativo Allegato B)

AGGIORNAMENTO

MARZO 2011

INDICE

ALLEGATI:

1) Informativa Generale (Art. 13 DLGS 196/2003)
2) Nomina del Responsabile del Trattamento dei dati personali
3) Nomina dell'Incaricato del Trattamento dei dati personali
4) Informativa sintetica Privacy (Art. 13 DLGS 196/2003) adattabile alla MODULISTICA COMUNALE
5) **Policy privacy** sito web
6) **Nomina dell'Amministratore di Sistema**
7) Richiesta a **Fornitore di attività esterne** della Dichiarazione di rispetto delle misure minime di sicurezza previste dall'Allegato B del DLGS. 196/03
8) Richiesta a **Fornitore di attività interne** della Dichiarazione di rispetto delle misure minime di sicurezza previste dall'Allegato B del DLGS. 196/03
9) Richiesta della **Dichiarazione di compatibilità tecnologica** delle attrezzature e programmi informatici
10) **Autorizzazione di accesso ai locali** dei soggetti ammessi agli archivi dopo l'orario di chiusura
11) Cartello per **Videosorveglianza**

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
per la
PROTEZIONE DEI DATI PERSONALI
IN MATERIA DI "MISURE MINIME" DI SICUREZZA

(ai sensi degli artt. 31-36 del D.Lgs. n. 196/2003 e del relativo Allegato B)

1. INTRODUZIONE E VARIAZIONI INTERVENUTE

Il presente Documento Programmatico sulla Sicurezza (DPS) costituisce **l'aggiornamento per il 2011** del DPS già adottato per l'anno precedente ed è stato redatto dal Comune di Castilenti, provincia di Teramo, sulla base delle indicazioni contenute nella "Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)" predisposta dal Garante per la Protezione dei dati personali.

Il DPS è stato aggiornato attraverso le informazioni rese dai "Responsabili per il trattamento dei dati personali" con la consulenza del Dott. Igino Addari che ne ha curato la stesura.

Nel corso dell'anno, da Aprile 2010 a Marzo 2011, si è proceduto a verificare se, nell'arco dei dodici mesi intercorsi dalla stesura del precedente Documento Programmatico sulla Sicurezza (DPS), si sono evidenziati rischi o minacce incombenti sul trattamento dei dati personali, in modo da prevedere interventi e misure di protezione.
Si è proceduto a sensibilizzare gli incaricati sulle misure da adottare per la lotta alla criminalità informatica, ai sensi della "Legge 18 marzo 2008, n. 48

Sono state prese in esame le disposizioni di cui al provvedimento del Garante per la protezione dei dati personali sulle "Semplificazione al modello per la notificazione al Garante" del 22 ottobre 2008, in G.U. n. 287 del 9 dicembre 2008.

Sono state impartite istruzioni sul provvedimento del Garante per la protezione dei dati personali in merito ai "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008, in G.U. n. 287 del 9 dicembre 2008

Sono stati attuati gli atti previsti dal provvedimento del Garante per la protezione dei dati personali dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008

La ricognizione della modalità di trattamento dei dati personali con sistemi elettronici è stata effettuata sulla base dell'analisi dei rischi, dell'attribuzione dei compiti e delle responsabilità nell'ambito delle Unità Operative cui è assegnato il trattamento stesso.
La ricognizione della modalità di trattamento dei dati personali, effettuata senza l'ausilio di strumenti elettronici, è stata finalizzata alla rilevazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative, all'applicazione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti e alla attuazione di

procedure per la conservazione di determinate categorie di atti in archivi ad accesso selezionato con l'identificazione degli incaricati.

Nel presente documento sono, quindi, esposte le misure di sicurezza aggiornate individuate dal COMUNE DI CASTILENTI (Provincia di Teramo) in ottemperanza a quanto disposto dal D.Lgs. del 30.06.2003 n. 196.
Si tratta cioè delle misura minime di sicurezza, così come delineate nel disciplinare tecnico contenuto nell'allegato B) della D.Lgs. 196/2003.
Tali misure coincidono con quelle ad oggi attuabili, sulla scorta:

- delle innovazioni tecnologiche o modificazioni di processi organizzativi aziendali;
- del monitoraggio delle procedure, della struttura organizzativa, logistica e tecnica;
- delle conoscenze acquisite;
- delle specifiche competenze interne;
- delle risorse umane disponibili;
- della programmazione economico-finanziaria dell'Ente;
- dell'adeguamento strutturale di aree e locali da realizzare garantendo la continuità del servizio pubblico;

così da ridurre al minimo:

- i rischi di distruzione o perdita dei dati;
- di accesso non autorizzato ai medesimi;
- di trattamento non consentito o non conforme.

Le misure adottate saranno oggetto di controllo e verifica periodica nel corso dell'anno.

Gli specifici interventi organizzativi e tecnici posti in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia non garantiscono la protezione dei dati personali senza tutte quelle attività di verifica e controllo nel tempo, essenziali per valutarne l'efficacia.

Senza procedure di controllo periodico, infatti, nessuna misura di protezione può essere considerata completa.

Le disposizioni contenute nel presente Documento Programmatico sulla Sicurezza sono adeguate, con cadenza annuale entro il 31 marzo, in esito alla verifica dell'efficacia delle misure di sicurezza in esso determinate, nonché in relazione alle modificazioni delle misure minime individuate secondo il disciplinare tecnico contenuto nell'allegato B) del D.Lgs. n. 196/2003, ed in relazione all'evoluzione tecnica
e all'esperienza maturata.

GUIDA ALLA LETTURA

Il DPS costituisce un documento programmatico e riporta, pertanto, tutte le misure minime, nonché quelle ritenute idonee, adottate e da adottare per la tutela dei dati personali. In concordanza con la sua esplicita natura, costituisce un documento *"in progress"*, soggetto a continui aggiornamenti con riferimento a nuovi trattamenti intrapresi, nuove misure adottate e a nuove norme emanate nel settore.

È articolato in **capitoli numerati** con relativi paragrafi e tabelle corredate di legenda, conformemente alle indicazioni e alle linee guida emanate dal Garante della Privacy.

I capitoli da 1 a 5 trattano il quadro di riferimento normativo che viene aggiornato in conseguenza dell'emanazione di nuove norme e disposizioni in materia.

I capitoli 6 e 7 sviluppano i punti obbligatori previsti dalla regola 19 dell'allegato B, "Disciplinare tecnico in materia di misure minime di sicurezza" , al "Codice in materia di protezione dei dati personali".

Il capitolo 6, in particolare, riporta le informazioni e le misure di sicurezza adottate o da adottare per il trattamento dei dati personali con supporti analogici (carta, video, nastri, ecc.)

Il capitolo 7, nello specifico, riporta le informazioni e le misure di sicurezza adottate o da adottare per il trattamento dei dati personali con strumenti elettronici oltre a misure obbligatorie di carattere generale quali la formazione, i trattamenti affidati a strutture esterne, l'idoneità di attrezzature e programmi utilizzati.

In appendice vengono riportati gli allegati che sono relativi alla modulistica, a nomine, delibere e qualsiasi altro atto da adottare per l'applicazione delle misure di sicurezza previste dal DPS.

2. DEFINIZIONI

Ai fini del presente Documento si intende:

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovraintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione;

BANCA DATI : qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

BLOCCO: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

DATO ANONIMO: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

DATI COMUNI: quelli che non rientrano nella categoria dei dati sensibili e giudiziari, quali: nome, cognome, telefono, fax, codice fiscale, partita Iva, ecc.

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;

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato;

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;

DATO PERSONALE: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

INCARICATO: la persona fisica incaricata, per iscritto, di compiere le operazioni di trattamento da parte del Responsabile e che opera sotto la sua diretta autorità;

INTERESSATO: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

MISURE MINIME: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di cui all'art. 31 del D.Lgs. n. 196/2003;

POSTA ELETTRONICA: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

RESPONSABILE: Il Responsabile della Unità Organizzativa aziendale, nominato ai sensi dell'art. 29 della Legge n. 196/2003, al quale spetta la responsabilità di qualsiasi trattamento dei dati personali operato nell'Unità cui è preposto, sia manuale che informatizzato, di carattere, amministrativo, gestionale, contabile o altro, nonché della sicurezza organizzativa, fisica e logica delle banche dati, nello svolgimento delle funzioni istituzionali del Comune di Castilenti e nei limiti stabiliti dalla legge e dai regolamenti;

RESPONSABILE DELLA GESTIONE DELLE ABILITAZIONI: il soggetto cui è conferito il compito di assegnare e revocare i "codici personali utenti" e le corrispondenti "parole chiave" (password).

STRUMENTI: i mezzi elettronici o comunque automatizzati con cui è effettuato il trattamento;

TITOLARE: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

TRATTAMENTO: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

3. QUADRO NORMATIVO DI RIFERIMENTO

Il Codice entrato in vigore il 1° gennaio 2004 ha confermato e aggiornato la disciplina in materia di sicurezza dei dati personali e dei sistemi informatici e telematici introdotta nel 1996.

Diversi principi affermati dal nuovo Codice non sono nuovi per gli operatori.

In particolare è stato confermato il principio (evidenziato con maggiore chiarezza dalle nuove disposizioni) secondo cui le "misure minime", di importanza tale da indurre il legislatore a prevedere anche una sanzione penale, sono solo una parte degli accorgimenti obbligatori in materia di sicurezza (art. 33 del Codice).

In materia, come già previsto dalla legge n. 675/1996, si distinguono *due distinti obblighi*:

a) l'obbligo più generale di ridurre al minimo determinati rischi.

Occorre custodire e controllare i dati personali oggetto di trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito.

Resta in vigore, oltre alle cosiddette "misure minime", l'obbligo di adottare ogni altra misura di sicurezza idonea a fronteggiare le predette evenienze, avuto riguardo alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, di cui si devono valutare comunque i rischi (art. 31).

Come in passato, l'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati; viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice), ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice);

b) nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le "misure minime".

Nel quadro degli accorgimenti più ampi da adottare per effetto dell'obbligo ora richiamato, occorre assicurare comunque un livello minimo di protezione dei dati personali.

Pertanto, in aggiunta alle conseguenze appena ricordate, il Codice conferma l'impianto secondo il quale l'omessa adozione di alcune misure indispensabili ("minime"), le cui modalità sono specificate tassativamente nell'Allegato B) del Codice, *costituisce anche reato* (art. 169 del Codice, che prevede l'arresto sino a due anni o l'ammenda da 10 mila euro a 50 mila euro, e l'eventuale "ravvedimento operoso" di chi adempie puntualmente alle prescrizioni impartite dal Garante una volta accertato il reato ed effettua un pagamento in sede amministrativa, ottenendo così l'estinzione del reato).

Il Codice, come previsto dalla legge n. 675/1996 e come dovrà avvenire periodicamente in base all'evoluzione tecnologica (art. 36 del Codice), ha *aggiornato l'elenco* delle "misure minime" le cui modalità di applicazione, sulla base di alcune prescrizioni di ordine generale (artt. 33-35 del Codice), sono indicate analiticamente nelle 29 regole incluse nell'Allegato B) del medesimo Codice.

Analogamente a quanto avveniva in passato, *le misure minime sono diverse* a seconda che il trattamento sia effettuato o meno con strumenti elettronici, oppure riguardi dati sensibili o giudiziari.

Le misure minime devono essere adottate conservando il documento a data certa il quale non va trasmesso al Garante, che può però richiederne l'esibizione in sede di accertamento anche ispettivo (artt. 157 ss. del Codice).

Per quanto riguarda le modalità per far risultare una "data certa" si dovrà applicare la disciplina civilistica in materia di prova documentale (v. in particolare, gli artt. 2702-2704 del codice civile) e si potranno tenere presenti i suggerimenti formulati dal Garante in un parere del 2000, e redatto a proposito di un analogo documento previsto in tema di sicurezza (art. 1l. n. 325/2000).

Per quanto riguarda le modalità per far risultare una "data certa" si dovrà applicare la disciplina civilistica in materia di prova documentale (v. in particolare, gli artt. 2702-2704 del codice civile) e si potranno tenere presenti i suggerimenti formulati dal Garante in un parere del 2000, e redatto a proposito di un analogo documento previsto in tema di sicurezza (art. 1l. n. 325/2000).

Il Garante richiama l'attenzione dei titolari del trattamento sulle seguenti possibilità utilizzabili per il rilevamento della "data certa":

a) ricorso alla c.d. "autoprestazione" presso uffici postali prevista dall'art. 8 del d.lg. 22 luglio 1999, n. 261, con apposizione del timbro direttamente sul documento avente corpo unico, anziché sull'involucro che lo contiene;

b) in particolare per le amministrazioni pubbliche, adozione di un atto deliberativo di cui sia certa la data in base alla disciplina della formazione, numerazione e pubblicazione dell'atto;

c) apposizione della c.d. marca temporale sui documenti informatici (art. 15, comma 2, legge 15 marzo 1997, n. 59; d.P.R. 10 novembre 1997, n. 513; artt. 52 ss. d.P.C.M. 8 febbraio 1999);

d) apposizione di autentica, deposito del documento o vidimazione di un verbale, in conformità alla legge notarile; formazione di un atto pubblico;

e) registrazione o produzione del documento a norma di legge presso un ufficio pubblico.

1. **L'art. 31 del D.Lgs. n. 196/2003**stabilisce che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da 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;

2. **L'art. 33 del D.Lgs. n. 196/2003**stabilisce che , i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

3. **L'art. 34 del D.Lgs. n. 196/2003** stabilisce che qualora il trattamento di dati sensibili sia realizzato mediante strumenti elettronici, devono essere rispettate le misure minime previste dal disciplinare tecnico contenuto nell'allegato B) della legge stessa, e che quindi deve essere predisposto e aggiornato con cadenza annuale un documento programmatico sulla sicurezza dei dati finalizzato alla definizione dei sottoelencati elementi, sulla base dell'analisi dei rischi, dell'attribuzione dei compiti e delle responsabilità nell'ambito delle Unità Operative deputate al trattamento dei dati stessi:

a) i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
b) i criteri e le procedure per assicurare l'integrità dei dati;
c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni d'accesso per via telematica;
d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

4. **L'art. 35 del D.Lgs. n. 196/2003** regola i "***Trattamenti senza l'ausilio di strumenti elettronici***" e 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.

5. **L'art. 36 del D.Lgs. n. 196/2003** in termini di "***Adeguamento***" stabilisce che:
Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

6. Il DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA di cui all'**ALLEGATO B del D.Lgs. n. 196/2003** stabilisce che entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige, anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza.

Sono state successivamente emanate le seguenti norme che hanno apportato integrazioni e modifiche alle disposizioni citate.

Sono state successivamente emanate le seguenti norme che hanno apportato integrazioni e modifiche alle disposizioni citate.

Delibera n. 13 del 1° marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet**"** *Gazzetta Ufficiale n. 58 del 10 marzo 2007.*

Delibera del Garante per la Protezione dei Dati Personali n° 17 del 19/04/2007, recante ad oggetto "*Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali*".

Deliberazione n. 23 del 14 giugno 2007 "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" - *(G.U. 13 luglio 2007, n. 161).*

Regolamento approvato con decreto del ministro dell'economia e delle finanze 18 gennaio 2008, n. 40, relativo alle "modalità di attuazione dell'articolo 48-bis del decreto del presidente della repubblica 29 settembre 1973, n. 602, recante disposizioni in materia di pagamenti da parte delle pubbliche amministrazioni".

Legge 18 marzo 2008, n. 48 - Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno.

Decreto Legislativo 30 maggio 2008, n. 109 "Attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE" in G.U. n. 141 del 18 giugno 2008.

Il provvedimento del Garante per la protezione dei dati personali dal titolo "Semplificazione al modello per la notificazione al Garante" del 22 ottobre 2008 , in G.U. n. 287 del 9 dicembre 2008.

Il provvedimento del Garante per la protezione dei dati personali dal titolo "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008, in G.U. n. 287 del 9 dicembre 2008.

Il provvedimento del Garante per la protezione dei dati personali dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008.

Art. 44 Legge 27 febbraio 2009, n. 14, conversione con modificazioni del decreto-legge 30 dicembre 2008, n. 207, Disposizioni in materia di tutela della riservatezza (Codice art. 13- Informativa)
1-bis - *I dati personali presenti nelle banche dati costituite sulla base di elenchi telefonici formati prima del 1° agosto 2005 sono lecitamente utilizzabili per fini promozionali sino al 31 dicembre 2009, anche in deroga agli articoli 13 e 23 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, dai soli titolari del trattamento che hanno provveduto a costituire dette banche dati prima del 1° agosto 2005.*

Art. 4, c. 9, Legge 4 marzo 2009, n. 15 "Delega al Governo finalizzata all'ottimizzazione della produttività del lavoro pubblico e alla efficienza e trasparenza delle pubbliche amministrazioni nonché disposizioni integrative delle funzioni attribuite al Consiglio nazionale dell'economia e del lavoro e alla Corte dei conti" in G.U. n. 53 del 5 marzo 2009, (Codice art. 1- Diritto alla protezione dei dati personali).

La Direttiva n. 2 del 26 maggio 2009 del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri sull'utilizzo di internet e della casella di posta elettronica certificata sul luogo di lavoro.

4. AMBITO DI APPLICAZIONE

Il documento in oggetto, nell'ambito delle attività svolte dalle Unità Operative e a fronte delle misure di sicurezza previste dall'art. 33 della Legge 30.06.2003 n.196, nonché degli standard minimi delineati dall'Allegato B alla medesima, intende definire gli elementi di riferimento necessari per l'adozione, l'adeguamento, lo sviluppo, l'implementazione gestionale di misure di sicurezza relative a:

a) trattamenti di dati personali (riferiti a dati comuni, senza particolare rilevanza caratteristica), di dati personali sensibili e giudiziari definiti all'art. 4 comma 1 lettere d) ed e), trattati con riguardo a quanto previsto dagli artt. 34 e 35 della Legge n. 196/2003;

b) gestione di archivi cartacei (correnti, di deposito, storici) e dei dati in essi contenuti

c) gestione di banche dati conservate su supporti informatizzati-automatizzati (memorie di rete, hard-disk, nastri, cd-rom, dvd, floppy disk);

d) gestione di archivi contenenti documenti particolari.

5. TITOLARE

Per tutti i trattamenti effettuati presso il COMUNE DI CASTILENTI, in conformità a quanto previsto dall'art. 28 del D.Lgs. n. 196 del 30.06.2003, il Titolare è il COMUNE DI CASTILENTI, legalmente rappresentato dal Sindaco *pro tempore*, ai sensi del vigente Statuto comunale.

Il Titolare del trattamento dei dati provvede ad impartire le istruzioni necessarie all'adozione, da parte dei Responsabili, di misure di sicurezza al fine di ridurre al minimo e prevenire:

a) i rischi di distruzione, perdita dei dati o danneggiamento, anche accidentale, degli Archivi cartacei ed elettronici, delle Banche Dati;

b) l'accesso non autorizzato nei locali ove gli Archivi e le Banche Dati sono collocati;

c) il trattamento non consentito o non conforme alle finalità della raccolta;

d) l'uso improprio dei dati in caso di cessazione del trattamento.

RELAZIONE ACCOMPAGNATORIA AL BILANCIO D'ESERCIZIO

Le scelte di fondo sulle modalità di trattamento sotto il profilo della sicurezza competono alle persone e agli organi legittimati ad adottare decisioni ed esprimere a vari livelli, in base al proprio ordinamento interno, la volontà della società, ente o altro organismo titolare del trattamento (art. 4, comma 1, lett. f), del Codice).
In questo quadro, il Codice ha introdotto una nuova regola per rendere meglio edotti gli organi di vertice del titolare del trattamento e responsabilizzarli in materia di sicurezza, attraverso l'obbligo di riferire nella relazione di accompagnamento a ciascun bilancio di esercizio circa l'avvenuta redazione o aggiornamento del DPS che sia obbligatorio come misura "minima" o che sia stato comunque adottato (regola 26 Allegato B).
Anche questa menzione rappresenta una misura "minima" nuova, indicata tra quelle di "tutela e garanzia" (regole 25 e 26 Allegato B).
In base alle disposizioni di Legge, si è provveduto, pertanto, alla **revisione del sistema di sicurezza**, ed all'aggiornamento del Documento Programmatico sulla Sicurezza verificando l'adozione delle misure minime previste dall'allegato B al Codice e valutando di non dover adottare altre misure diverse da quelle già in essere.

6. DATI TRATTATI CON SISTEMI CARTACEI

TRATTAMENTO DI DATI MEDIANTE STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI

1. I Responsabili nel designare per iscritto gli incaricati e nell'impartire le istruzioni, ai sensi dell'art. 30 del D.Lgs. n. 196/2003, devono prescrivere che i soggetti designati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti loro assegnati.

2. Gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni eseguite.

3. Nel caso di dati “sensibili" o di “natura giudiziaria”, di cui rispettivamente all’art. 4 comma 1 lettere d) ed e) del D.Lgs. n. 196/2003, oltre alle misure di cui ai punti 1 e 2 del seguente articolo, devono essere osservate le seguenti modalità:

a) se affidati agli incaricati, gli atti e i documenti concernenti i dati vanno conservati, sino alla restituzione, in contenitori muniti di serratura;
b) l'accesso agli archivi va controllato e devono essere identificati e registrati i soggetti che vi accedono dopo l'orario di chiusura degli archivi stessi.

4. Le medesime modalità di cui al precedente punto 3, si applicano alla conservazione anche di altri tipi di supporti analogici (video, nastri di registrazione ecc.) contenenti la riproduzione di informazioni relative al trattamento dei dati di cui al citato art.. 4 comma 1 lettere d) ed e) della D.Lgs. n. 196/2003

6.1 Elenco dei trattamenti di dati personali con il sistema cartaceo

Gli archivi cartacei sono quelli detenuti dall'Ente e che generano:

- l'Archivio Corrente (pratiche aperte)
- l'Archivio di Deposito (pratiche concluse)
- l'Archivio Storico (pratiche concluse da oltre 40 anni)

Il Sig. ANTONIO LEONE è stato nominato Responsabile e incaricato del Servizio per la Tenuta del Protocollo informatico, della gestione dei flussi documentali e degli Archivi (art. 61 DPR 445/2000).

E' stato adottato il Manuale di Gestione del protocollo informatico e del Servizio archivistico e il Nuovo Titolario per i Comuni. La relativa delibera è stata pubblicata all'ALBO PRETORIO.

Il Responsabile/Incaricato del Protocollo informatico esegue le operazioni di registrazione della corrispondenza in un locale che prevede la restrizione fisica all'accesso in quanto dette operazioni vengono svolte isolandone la postazione attraverso una porta d'accesso munita di serratura.
La distribuzione della corrispondenza in Entrata, a cura dello stesso Responsabile/Incaricato, viene effettuata ponendo la documentazione all'interno di singole cartelle da consegnare al Responsabile dell'U.O.R. destinataria e la corrispondenza, contenente dati sensibili e/o giudiziari, viene consegnata al destinatario in busta chiusa.

L'archivio Corrente è tenuto c/o le diverse U.O.R. e prevede la restrizione fisica per l'accesso in quanto i dati sensibili e giudiziari dell'archivio corrente sono conservati in armadi muniti di serratura e chiusi a chiave.

L'archivio di deposito e l'archivio storico sono separati dall'archivio corrente e tenuti in un apposito locale con porta d'accesso munita di serratura.

Si riporta la tabella riepilogativa, delle informazioni di base relative ai dati personali trattati col sistema cartaceo, contenente le seguenti informazioni:

1) *Identificativo del trattamento:* codice identificativo relativo a ciascun trattamento.
2) *Descrizione sintetica:* descrive il trattamento dei dati.
3) *Natura dei dati trattati:* riporta se, tra i dati oggetto del singolo trattamento elencato, sono presenti dati sensibili o giudiziari, oltre ad altri dati personali.
4) *Struttura di riferimento:* indica la macro-struttura all'interno della quale viene realizzato il trattamento.
5) *Altre funzioni che concorrono al trattamento:* indica, oltre quella che primariamente detiene la responsabilità dell'attività, anche strutture, interne od esterne, che concorrono all'organizzazione del titolare.
6) *Descrizione degli strumenti utilizzati:* indica, il supporto cartaceo, o comunque analogico, sul quale sono conservati i dati.

Tabella 1.1 **Archivio cartaceo**: informazioni di base

Identificativo Trattamento **Archivio cartaceo**	Descrizione sintetica	Natura dei dati trattati	Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
1	PERSONALE (STATO GIURIDICO)-	Sensibili	UFFICIO AMMINISTRATIVO		MODULI CARTACEI
2	ANAGRAFE - STATO CIVILE - ELETTORALE - COMMERCIO - SERVIZI SOCIALI	Giudiziari	UFFICIO AMMINISTRATIVO	PREFETTURA - UFFICI GIUDIZIARI E CONSOLARI	MODULI CARTACEI
3	PERSONALE (GESTIONE ECONOMICA) - TRIBUTI- CONTRIBUENTI - DIRITTO STUDIO - PROGRAMMAZIONE ECONOMICO FINANZIARIA	Comuni	UFFICIO FINANZIARIO	CONCESSIONARIO RISCOSSIONE	MODULI CARTACEI
4	EDILIZIA - URBANISTICA - LLP	Giudiziari	UFFICIO TECNICO	AUTORITA' DI VIGILANZA LLPP - PREFETTURA	SCHEDE
5	VIGILANZA STRADALE - ALBO PRETORIO - POLIZIA AMMINISTRATIVA	Giudiziari	UFFICIO AMMINISTRATIVO	QUESTURA - PREFETTURA - MOTORIZZAZIONE	MODULI VARI
6	VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI	Giudiziari	UFFICIO POLIZIA MUNICIPALE	QUESTURA - PREFETTURA - UFFICI GIUDIZIARI	MODULI VARI
Data di aggiornamento: 23/03/2011					

6.2 Distribuzione dei compiti e delle responsabilità dei dati trattati con il sistema cartaceo

Si riporta la tabella riepilogativa, dei dati relativi alle strutture preposte al trattamento dell'Archivio cartaceo, contenente le seguenti informazioni:

Identificativo Struttura Trattamento: contiene lo stesso identificativo utilizzato nella precedente Tab. 1.1.

Responsabile della struttura: indica il responsabile della struttura.

Trattamenti operati e compiti della struttura dalla struttura: riporta i trattamenti per i quali la struttura ha la primaria responsabilità.
Nei compiti assegnati alla struttura la dicitura "Tutti" include tutti i tipi di trattamento quali: acquisizione dei dati, consultazione, comunicazione a terzi e conservazione, oltre quelli di carattere aggiuntivo per la definizione della pratica gestita.

Tipo Archivio: riporta la tipologia di Archivio sul quale viene effettuato il trattamento (Corrente/Deposito/Storico - Tutti)

Tabella 2.1 Strutture preposte ai trattamenti dell'**Archivio cartaceo**

Identificativo Trattamento **Archivio cartaceo**	Responsabile Struttura	Trattamenti e compiti dalla struttura	Tipo Archivio
1	LEONE ANTONIO	Tutti	Corrente Tutti
2	LEONE ANTONIO	Tutti	Corrente Tutti
3	LANCIANESE NICOLINO	Tutti	Corrente Deposito
4	LUPINETTI BIAGIO	Tutti	Corrente Deposito
5	LEONE ANTONIO	Tutti	Corrente Deposito
6	LUPINETTI BIAGIO	Tutti	Corrente Deposito
Data di aggiornamento: 23/03/2011			

6.3 Responsabili dei trattamenti con il sistema cartaceo

In conformità con le disposizioni previste dal D.Lgs. n. 196 del 30.06.2003 vengono individuati, quali Responsabili dei trattamenti, le seguenti figure:
a) i Responsabili delle singole Unità Organizzative per i trattamenti, informatizzati o manuali, che risultano direttamente gestiti dalle Unità Organizzative medesime come di seguito riportato.

I Responsabili del trattamento dei dati coincidono con i responsabili dei servizi cui fanno capo le strutture preposte ai trattamenti e sono stati nominati con deliberazione del Consiglio Comunale n. 2 del 26/01/2000 avente per oggetto: "Adozione del regolamento per il trattamento dei dati personali – L. 675/96 – D.LGS. 135/99".

I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare ai sensi dell'art. 29 del D.Lgs. 196/2003.

Tabella 2.2 Responsabili del trattamento dati su documenti cartacei

Identificativo Trattamento **Archivio cartaceo**	Responsabile Trattamento	Trattamenti operati dalla struttura
1 + 2 +5	LEONE ANTONIO	PERSONALE (STATO GIURIDICO)- ANAGRAFE - STATO CIVILE - ELETTORALE - COMMERCIO - SERVIZI SOCIALI VIGILANZA STRADALE - ALBO PRETORIO - POLIZIA AMMINISTRATIVA
3	LANCIANESE NICOLINO	PERSONALE (GESTIONE ECONOMICA) - TRIBUTI- CONTRIBUENTI - DIRITTO STUDIO - PROGRAMMAZIONE ECONOMICO FINANZIARIA
4 + 6	LUPINETTI BIAGIO	EDILIZIA - URBANISTICA - LLP VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI
Data di aggiornamento: 23/03/2011		

6.4 Incaricati dei trattamenti con il sistema cartaceo

Gli **Incaricati** del trattamento dei dati contenuti su documenti cartacei sono stati individuati dai Responsabili del trattamento ai sensi della deliberazione del Consiglio Comunale n. 2 del 26/01/2000 avente per oggetto: "Adozione del regolamento per il trattamento dei dati personali – L. 675/96 – D.Lgs. 135/99".

Tabella 2.3 Incaricati del trattamento dei dati su documenti cartacei

Identificativo Trattamento **Archivio cartaceo**	Incaricati Trattamento	Trattamenti operati dalla struttura
1 + 2	1. LEONE ANTONIO	PERSONALE (STATO GIURIDICO)- ANAGRAFE - STATO CIVILE - ELETTORALE - COMMERCIO - SERVIZI SOCIALI
3	2. LANCIANESE NICOLINO	PERSONALE (GESTIONE ECONOMICA) - TRIBUTI- CONTRIBUENTI - DIRITTO STUDIO - PROGRAMMAZIONE ECONOMICO FINANZIARIA
4 + 6	3. LUPINETTI BIAGIO	EDILIZIA - URBANISTICA - LLP VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI
5	LEONE ANTONIO 4. DI DONATO ANTONIO	VIGILANZA STRADALE - ALBO PRETORIO - POLIZIA AMMINISTRATIVA
Data di aggiornamento: 23/03/2011		

6.5 Analisi dei rischi dei trattamenti con il sistema cartaceo

L'analisi dei rischi ha permesso di individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati elettronici.

La relativa valutazione delle possibili conseguenze e il grado di gravità, così come sono state rilevate, impone l'adozione di adeguate misure di protezione.

Si riporta la tabella riepilogativa dell'analisi dei rischi, che incombono sul trattamento dei dati personali gestiti in forma cartacea, contenente le seguenti informazioni:

1) *Elenco degli eventi:* contiene l'elenco degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali.

2) *Impatto sulla sicurezza dei dati:* contiene la descrizione delle principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento ed una valutazione della gravità delle stesse, anche in relazione alla probabilità stimata dell'evento. L'indicatore di gravità è suddiviso su quattro livelli: alta/media/bassa/zero.

3) *Rif. misure d'azione:* contiene il riferimento alle contromisure adottata o programmate.

Tabella 3.1c - Archivi cartacei: Analisi dei rischi

Evento		Impatto sulla sicurezza dei dati		Rif. misure d'azione (contromisure)
		Descrizione	Gravità stimata	
Comportamenti degli operatori				
	carenza di consapevolezza, disattenzione o incuria	Sottrazione o perdita dei dati	alta	Formazione, Note e circolari periodiche
	errori materiali	Dati errati e non corrispondenze	media	Processi di controllo e verifiche
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	Sottrazione o indebita diffusione di dati	media	Controllo autorizzazioni e strumenti di identificazione
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati	media	Sistemi antincendio e digitalizzazione archivi
	errori umani nella gestione della sicurezza fisica	Sottrazione o perdita dei dati	media	Distribuzione di compiti e funzioni di sicurezza incrociate
Data aggiornamento: 23/03/2011				

7. DATI TRATTATI CON SISTEMI ELETTRONICI

RISORSE SOFTWARE E HARDWARE

Le Banche Dati e gli archivi elettronici risiedono su n. 1 Server dotato del Sistema Operativo Windows 2000.

Al Server sono collegati in rete n. 9 PC Client sui quali operano gli incaricati.
N. 6 postazioni sono dotate del Sistema Operativo Windows 98, N. 3 postazioni sono dotate del Sistema Operativo Windows XP PRO.

TRATTAMENTO DI DATI MEDIANTE PROCEDURE INFORMATIZZATE DEL SISTEMA INFORMATIVO COMUNALE

1. I Responsabili, nominati ai sensi dell'art. 29 della Legge n. 196/2003, provvedono per iscritto alla designazione dei soggetti incaricati, da abilitarsi all'uso delle procedure informatizzate, specificando per ciascuno a quali funzioni/insiemi di dati debbono essere in grado di accedere. I Responsabili, con le medesime modalità, impartiscono agli incaricati le necessarie istruzioni per il corretto utilizzo di dette procedure.
   Il soggetto Responsabile della gestione delle abilitazioni provvede ai propri compiti con le seguenti modalità:

a) a ciascun incaricato che, per esigenze di servizio, deve poter utilizzare una procedura informatizzata ed accedere di conseguenza alle informazioni contenute negli archivi della stessa, è assegnato un "codice personale utente" ed una "parola chiave" segreta (password) individuale e riservata in modo esclusivo.
b) ciascun incaricato, per mezzo di detto codice di accesso, è abilitato all'utilizzo delle funzionalità necessarie allo svolgimento delle attività allo stesso assegnate e può contemporaneamente accedere ai soli dati strettamente necessari allo scopo.

2. Ciascuna procedura informatizzata deve essere strutturata in modo da consentire di:

a) segmentare le abilitazioni di accesso ed utilizzo in base alle necessità dell'unità operativa,
b) individuare a posteriori l'autore di ciascuna operazione effettuata sui dati trattati. Il rispetto dei requisiti di cui al presente punto 2 deve essere garantito anche dal fornitore o dal produttore di ciascuna procedura informatizzata.

3. E' fatto obbligo a ciascun incaricato di non comunicare ad altri il proprio codice identificativo personale, né la parola chiave (password) segreta, di non lasciare la stazione di lavoro situata al proprio posto di lavoro collegata ed incustodita, di non utilizzare i dati consultabili per fini non strettamente attinenti alle esigenze di servizio.

INTERNET PUBBLICAZIONE DATI PERSONALI

Vengono previste le diverse forme di accessibilità ad atti e documenti evitando, per quanto possibile, di applicare modalità indifferenziate che non tengano conto delle finalità sottostanti alla trasparenza, nonché delle diverse situazioni personali.

Viene fatto uso di nuove tecnologie che facilitano la conoscenza da parte dei cittadini, tenuto conto anche del diritto all'utilizzo nei loro confronti delle tecnologie telematiche *(art. 3 d.lg. 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale").*

Sono previste, ove necessario, forme di accesso in rete selezionato, attribuendo agli interessati una chiave personale (*username* e *password*; n. di protocollo o altri estremi identificativi di una pratica forniti dall'ente agli aventi diritto). Ad esempio, la pubblicità tramite siti web su talune procedure concorsuali può essere perseguita divulgando integralmente alcuni atti (ad es., deliberazioni che indicono concorsi o approvano graduatorie), indicando invece in sezioni dei siti ad accesso selezionato alcuni dettagli conoscibili da interessati e controinteressati (elaborati, verbali, valutazioni, documentazione personale comprovante titoli).

Accorgimenti analoghi sono previsti, a seconda dei casi, con riferimento alle graduatorie relative al riconoscimento di autorizzazioni, agevolazioni, benefici ed iniziative a vantaggio di categorie di cittadini (es., procedure per ammettere minori ad asili nido, per assegnare alloggi di edilizia residenziale pubblica, per valutare domande di mobilità o rilasciare autorizzazioni e concessioni edilizie).

Per quanto non riportato sul presente DPS si fa riferimento alle disposizioni previste dalla Deliberazione n. 17 del Garante della Privacy del 19 aprile 2007 .

AMMINISTRATORE DI SISTEMA

Il comune di Castilenti non ha nominato l'Amministratore di Sistema.

In relazione al Provvedimento del Garante per la protezione dei dati personali dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, in G.U. n. 300 del 24 dicembre 2008 l'Ente provvederà:

- a predisporre lettere di incarico e lista degli "amministratori di sistema" per i trattamenti in corso o iniziati dopo il 25 gennaio 2009, attività che verrà completata nei termini di legge previsti per il 30 giugno 2009 come da Comunicato stampa del Garante del 23 febbraio 2009;
- a richiedere alle società terze a cui sono affidati in outsourcing i trattamenti di dati personali la lista degli "amministratori di sistema" che gestiscono tali trattamenti e l'attestazione (per iscritto) che tali "amministratori" hanno le caratteristiche richieste dalla legge;
- a comunicare a tutto il personale (previa comunicazione via e-mail e/o intranet):
  - i contenuti del provvedimento del Garante,
  - l'elenco degli amministratori di sistema,
- a predisporre un "piano formativo" ad hoc per gli "amministratori di sistema";
- a predisporre un sistema di log per gli accessi effettuati dagli "amministratori di sistema".

Per l'individuazione e la designazione degli amministratori di sistema è necessario introdurre le seguenti misure e accorgimenti, per tutti i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella *Gazzetta Ufficiale* del citato provvedimento, al più presto e comunque entro, e non oltre, il termine di centoventi giorni dalla medesima data; per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.

a) Valutazione delle caratteristiche soggettive
L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

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

c) Elenco degli amministratori di sistema
Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i

titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in *G.U.* 10 marzo 2007, n. 58) sulle linee guida del Garante per la posta elettronica e internet o, in alternativa, mediante altri strumenti di comunicazione interna (*ad es., intranet* aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

d) Servizi in outsourcing
Nel caso di servizi di amministrazione di sistema affidati in ***outsourcing*** il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

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

f) Registrazione degli accessi
Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

Come previsto al punto 1 del citato provvedimento del Garante Privacy, sono individuabili diverse tipologie di **amministratori di sistema** (*system administrator*):

Sulla base di quanto riportato al punto precedente, sono individuabili, tre distinte tipologie di amministratori di sistema:

- **amministratore della rete** (*network administrator*) di telecomunicazioni, che gestisce le modalità di accesso alla rete aziendale, sia dall'interno sia dall'esterno, e le relative abilitazioni ai servizi di rete;
- **amministratore del server** (*database administrator*), ovvero dell'elaboratore su cui risiedono la base dati e le funzioni elaborative centralizzate di una procedura informatica;
- **amministratore di procedura**, che gestisce le modalità di accesso e le abilitazioni ad operare degli incaricati in relazione ai trattamenti che si avvalgono di una stessa procedura informatica.

Le diverse figure di Amministratore possono essere raggruppate in un unico soggetto “Amministratore di Sistema”.

Le attribuzioni di detti ruoli e la definizione dettagliata dei compiti e delle modalità operative assegnate possono essere così riassunte :
Amministratore di rete

- possessore dei codici e delle password di accesso per la configurazione degli apparati attivi per la trasmissione dei dati sulla rete;
- abilitato al rilascio dei codici e delle password da assegnarsi alle eventuali terze parti da abilitarsi al collegamento al sistema informatizzato aziendale dall'esterno (ad esempio, i fornitori di procedure informatiche ai fini di consentire l'erogazione dell'assistenza da remoto);
- incaricato di definire ed aggiornare, compatibilmente con le soluzioni disponibili sul mercato, gli strumenti tecnologici atti a proteggere la rete aziendale da intrusioni e accessi non autorizzati;
- incaricato di garantire il corretto funzionamento degli strumenti tecnologici acquisiti a tal fine;
- incaricato di svolgere controlli atti a rilevare eventuali accessi alla rete non autorizzati;
- incaricato di mantenere aggiornata la documentazione tecnica relativa alla configurazione hardware e software della rete e degli strumenti di sicurezza;
- copia di tutti i codici e relative password di accesso in possesso dell'amministratore di rete e degli schemi tecnici della rete deve essere consegnata e mantenuta aggiornata presso il Responsabile del Servizio Sistemi Informativi e Organizzazione.

Amministratore di server

- possessore dei codici e delle password di accesso per la configurazione del server e l'accesso alle funzioni sistemistiche di manutenzione della medesima;
- abilitato al rilascio dei codici e delle password da assegnarsi alle eventuali terze parti da abilitarsi al collegamento al server dall'esterno (ad esempio, i fornitori di procedure informatiche ai fini di consentire l'erogazione dell'assistenza da remoto);
- incaricato di definire ed aggiornare, compatibilmente con le soluzioni messe a disposizione dal produttore del software di sistema in uso, gli strumenti tecnologici atti a proteggere il server da intrusioni e accessi non autorizzati;
- incaricato di garantire il corretto funzionamento degli strumenti tecnologici acquisiti a tal fine;
- incaricato di svolgere controlli atti a rilevare eventuali accessi al server non autorizzati;
- incaricato di garantire l'effettuazione delle operazioni di salvataggio dei data base presenti sul server, la non accessibilità di tali copie da parte di terzi non autorizzati, l'efficacia delle procedure di ripristino in caso di danneggiamento dei dati, la distruzione delle copie non più necessarie per le finalità di ripristino;
- copia di tutti i codici e relative password di accesso in possesso dell'amministratore di server deve essere consegnata e mantenuta aggiornata presso il Responsabile del CED, se nominato.

Amministratore di procedura

- possessore dei codici e delle password di accesso all'intera base dati della procedura ed all'insieme completo delle funzionalità elaborative gestite dalla medesima;
- abilitato al rilascio dei codici e delle password da assegnarsi agli incaricati dei trattamenti che utilizzano la procedura;
- incaricato di assegnare a ciascun "incaricato del trattamento" il profilo di utenza corrispondente alle sole funzionalità necessarie alla attività istituzionale svolta dal medesimo;
- incaricato di garantire, compatibilmente con le caratteristiche tecnologiche della procedura gestita, che i codici di accesso assegnati non siano utilizzabili da più stazioni di lavoro contemporaneamente e che le relative password siano modificabili e conosciute soltanto dagli incaricati che ne sono in possesso;

- incaricato di garantire, compatibilmente con le caratteristiche tecnologiche della procedura gestita, che sia possibile individuare "a posteriori" il codice di accesso che ha effettuato una data operazione sui dati contenuti nel data base della procedura;
- copia di tutti i codici e relative password di accesso all'intera base dati in possesso dell'amministratore di procedura deve essere consegnata e mantenuta aggiornata presso il Responsabile del CED, se nominato.

SEMPLIFICAZIONE NOTIFICAZIONE

Con riferimento al Provvedimento del Garante per la protezione dei dati personali "Semplificazione al modello per la notificazione al Garante" del 22 ottobre 2008 , in G.U. n. 287 del 9 dicembre 2008, l'Ente non è tenuto alla notificazione dei propri trattamenti e dunque i contenuti di tale provvedimento non sono stati presi in considerazione.

Casi nei quali la notificazione è dovuta
In termini generali, la notificazione è dovuta per disposizione di legge esclusivamente da soggetti che effettuano trattamenti riguardanti:

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.

La notificazione relativa al trattamento dei dati sopra menzionati non è tuttavia dovuta se relativa all'attività dei medici di famiglia e dei pediatri di libera scelta, in quanto tale funzione è considerata tipica del loro rapporto professionale con il Servizio sanitario nazionale (art. 37, comma 1-*bis*, del Codice).
Sono stati, inoltre, disposti alcuni esoneri dall'obbligo di notificazione nei riguardi dei soggetti e dei trattamenti indicati in un'apposita deliberazione pubblicata sul sito Internet del Garante con chiarimenti in riguardo.

ROTTAMAZIONE PC ED AFFINI

Con riferimento al provvedimento del Garante per la protezione dei dati personali "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008, in G.U. n. 287 del 9 dicembre 2008, il Garante richiede che siano adottate appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possono verificarsi in occasione della **dismissione di apparati elettrici ed elettronici** (artt. 31 ss. del Codice).

In relazione a tale provvedimento l'Ente ha provveduto ad impartire istruzioni:

- sul "**Reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche**" che tengono conto di quanto indicato nell'allegato A del citato provvedimento.

In caso di reimpiego e riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche le misure e gli accorgimenti volti a prevenire accessi non consentiti ai dati personali in esse contenuti, adottati nel rispetto delle normative di settore, devono consentire l'effettiva cancellazione dei dati o garantire la loro non intelligibilità.
Tali misure, anche in combinazione tra loro, devono tenere conto degli standard tecnici esistenti e possono consistere, tra l'altro, in:

1. Cifratura di singoli *file* o gruppi di *file*, di volta in volta protetti con parole-chiave
2. Memorizzazione dei dati sui dischi rigidi (*hard-disk*) dei *personal computer* o su altro genere di supporto magnetico od ottico (cd-rom, dvd-r) in forma automaticamente cifrata;
3. Cancellazione sicura delle informazioni;
4. Formattazione "a basso livello" dei dispositivi di tipo *hard disk*
5. Demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici.

- sullo "**Smaltimento di rifiuti elettrici ed elettronici**" che tengono conto di quanto indicato nell'allegato B al provvedimento su citato.

La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali:

1. sistemi di punzonatura o deformazione meccanica;
2. distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd);
3. demagnetizzazione ad alta intensità.

CRIMINI INFORMATICI

Ai sensi di quanto stabilito dalla “Legge 18 marzo 2008, n. 48 - Ratifica ed esecuzione della Convenzione del Consiglio d’Europa sulla criminalità informatica, emanata a Budapest il 23 novembre 2001, e norme di adeguamento dell’ordinamento interno” che ha introdotto nuovi adempimenti per la sicurezza informatica in quanto ha modificato (art. 10) sia il “Codice in materia di protezione dei dati personali” sia (art. 7) il decreto legislativo 8 giugno 2001, n. 231, l’Ente:

- ha sensibilizzato, per iscritto (e-mail) tutto il personale sui nuovi requisiti di legge e sui comportamenti richiesti;
- sta valutando l’opportunità di predisporre un nuovo sistema di controllo interno coerente con i requisiti del decreto legislativo 8 giugno 2001, n. 231.

7.1 Elenco dei trattamenti di dati personali con sistemi elettronici

Si riporta la tabella riepilogativa, delle informazioni di base relative ai dati personali trattati con sistemi elettronici, contenente le seguenti informazioni:

1) *Identificativo del trattamento:* codice identificativo relativo a ciascun trattamento.
2) *Descrizione sintetica:* descrive il trattamento.
3) *Natura dei dati trattati:* riporta se, tra i dati oggetto del singolo trattamento elencato, sono presenti dati sensibili o giudiziari, oltre ad altri dati personali.
4) *Struttura di riferimento:* indica la macro-struttura all'interno della quale viene realizzato il trattamento.
5) *Altre funzioni che concorrono al trattamento:* indica, oltre quella che primariamente detiene la responsabilità dell'attività, anche strutture, interne od esterne, che concorrono all'organizzazione del titolare.
6) *Descrizione degli strumenti utilizzati:* indica, gli strumenti utilizzati per il trattamento e la conservazione dei dati.

Tabella 1.1. **Archivi elettronici**: informazioni di base

Identificativo Trattamento **Dati informatici**	Descrizione sintetica	Natura dei dati trattati	Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
1	PERSONALE (STATO GIURIDICO)-	Sensibili	UFFICIO AMMINISTRATIVO		PC
2	ANAGRAFE - STATO CIVILE - ELETTORALE - COMMERCIO - SERVIZI SOCIALI	Giudiziari	UFFICIO AMMINISTRATIVO	PREFETTURA - UFFICI GIUDIZIARI E CONSOLARI	PC COLLEGAMENTI TELEMATICI E SUPPORTI
3	PERSONALE (GESTIONE ECONOMICA) - TRIBUTI-CONTRIBUENTI - DIRITTO STUDIO - PROGRAMMAZIONE ECONOMICO FINANZIARIA	Comuni	UFFICIO FINANZIARIO	CONCESSIONARIO RISCOSSIONE	PC COLLEGAMENTI TELEMATICI E SUPPORTI
4	EDILIZIA - URBANISTICA - LLP	Giudiziari	UFFICIO TECNICO	AUTORITA' DI VIGILANZA LLPP - PREFETTURA	PC COLLEGAMENTI TELEMATICI E SUPPORTI
5	VIGILANZA STRADALE - ALBO PRETORIO - POLIZIA AMMINISTRATIVA	Comuni	UFFICIO AMMINISTRATIVO	QUESTURA - PREFETTURA - MOTORIZZAZIONE	PC COLLEGAMENTI TELEMATICI E SUPPORTI (PRA)
6	VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI	Giudiziari	UFFICIO POLIZIA MUNICIPALE	QUESTURA - PREFETTURA - UFFICI GIUDIZIARI	PC E SUPPORTI
Data di aggiornamento: 23/03/2011					

7.2 DESCRIZIONE DEGLI STRUMENTI UTILIZZATI PER IL TRATTAMENTO DI DATI PERSONALI

Si riporta la tabella riepilogativa degli strumenti utilizzati per il trattamento dei dati personali con sistemi elettronici:

1) *Identificativo del trattamento:* codice identificativo relativo a ciascun trattamento

2) *Banca dati:* l'identificativo della Banca dati o dell'archivio informatico in cui sono contenuti i dati che sono trattati.

3) *Ubicazione fisica dei supporti di memorizzazione:* contiene l'indicazione del luogo in cui risiedono fisicamente i dati

4) *Tipologia di dispositivi di accesso:* elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.

5) *Tipologia di interconnessione:* descrizione sintetica e qualitativa della rete informatica che collega i dispositivi d'accesso utilizzati dagli incaricati ai dati: rete locale, Extranet, Internet, ecc.

Tabella 1.2 - Descrizione degli strumenti utilizzati

Identificativo trattamento **Dati informatici**	Eventuale banca dati o Archivio informatico	Ubicazione fisica supporti di memorizzazione		Tipologia dispositivi di accesso	Tipologia interconnessione
1	PERSONALE (STATO GIURIDICO)-	Elaboratore	sede	PC	Rete locale
2	ANAGRAFE - STATO CIVILE - ELETTORALE - COMMERCIO - SERVIZI SOCIALI	Elaboratore	sede	PC	Rete locale Internet
3	PERSONALE (GESTIONE ECONOMICA) - TRIBUTI-CONTRIBUENTI - DIRITTO STUDIO - PROGRAMMAZIONE ECONOMICO FINANZIARIA	Elaboratore	sede	PC	Rete locale Internet
4	EDILIZIA - URBANISTICA - LLP	Elaboratore	sede	PC	Rete locale
5	VIGILANZA STRADALE - ALBO PRETORIO - POLIZIA AMMINISTRATIVA	Elaboratore	sede	PC	Rete locale
6	VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI	Elaboratore	sede	PC	Rete locale
Data di aggiornamento: 23/03/2011					

Note:

7.3 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

Viene riportata una mappa che associa ad ogni struttura i trattamenti da questa effettuati, con una sintetica descrizione organizzativa della struttura medesima e le relative responsabilità.

Si riporta la tabella riepilogativa delle strutture preposte al trattamento dei dati personali con sistemi elettronici, contenente le seguenti informazioni:

1) *Struttura aziendale:* contiene lo stesso identificativo utilizzato nella sezione precedente.

2) *Responsabile della struttura:* indica il nome del dirigente o del responsabile della struttura

3) *Trattamenti operati dalla struttura:* indica i trattamenti per i quali la struttura ha la primaria responsabilità.

4) *Compiti della struttura:* riporta una sintetica descrizione dei compiti assegnati alla struttura in ciascuno dei trattamenti di sua competenza.

Tabella 2.1 **Archivi elettronici**: Strutture preposte ai trattamenti

Identificativo Struttura Trattamento **Dati informatici**	Responsabile struttura (Servizio)	Trattamenti operati dalla struttura	Compiti della struttura
1 + 2	LEONE ANTONIO	PERSONALE (STATO GIURIDICO)- ANAGRAFE - STATO CIVILE - ELETTORALE - COMMERCIO - SERVIZI SOCIALI	Acquisizione e caricamento dei dati, modifiche, consultazione, stampe, comunicazione a terzi, salvataggi, ripristini
3	LANCIANESE NICOLINO	PERSONALE (GESTIONE ECONOMICA) - TRIBUTI- CONTRIBUENTI - DIRITTO STUDIO - PROGRAMMAZIONE ECONOMICO FINANZIARIA	Acquisizione e caricamento dei dati, modifiche, consultazione, stampe, comunicazione a terzi, salvataggi, ripristini
4	LUPINETTI BIAGIO	EDILIZIA - URBANISTICA - LLP	Acquisizione e caricamento dei dati, modifiche, consultazione, stampe, comunicazione a terzi, salvataggi, ripristini
5	LEONE ANTONIO	VIGILANZA STRADALE - ALBO PRETORIO - POLIZIA AMMINISTRATIVA VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI	Acquisizione e caricamento dei dati, modifiche, consultazione, stampe, comunicazione a terzi, salvataggi, ripristini
6	LUPINETTI BIAGIO	VIGILANZA STRADALE - ALBO PRETORIO - POLIZIA AMMINISTRATIVA VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI	Acquisizione e caricamento dei dati, modifiche, consultazione, stampe, comunicazione a terzi, salvataggi, ripristini
Data di aggiornamento: 23/03/2011			

Note:

7.4 Responsabili dei trattamenti con il sistema informatico

I Responsabili del trattamento dei dati coincidono con i responsabili dei servizi cui fanno capo le strutture preposte ai trattamenti.

I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare ai sensi dell'art. 29 del D.Lgs. 196/2003.

Si riporta la tabella riepilogativa dei Responsabili preposti al trattamento dei dati personali con sistemi elettronici, contenente le seguenti informazioni:

1) *Identificativo Struttura trattamento:* contiene lo stesso identificativo utilizzato per identificare l'Archivio o Banca Dati.

2) *Responsabile del trattamento:* indica il nome del dirigente o del responsabile del trattamento ai sensi dell'art. 29 del D.Lgs. 196/2003.

3) *Trattamenti operati dalla struttura:* indica i trattamenti per i quali la struttura ha la primaria responsabilità.

Tabella 2.2 Responsabili del trattamento di dati informatici

Identificativo Struttura Trattamento	Responsabile Trattamento	Trattamenti operati dalla struttura
1 + 2+5	LEONE ANTONIO	PERSONALE (STATO GIURIDICO)- ANAGRAFE - STATO CIVILE - ELETTORALE - COMMERCIO - SERVIZI SOCIALI VIGILANZA STRADALE - ALBO PRETORIO - POLIZIA AMMINISTRATIVA
3	LANCIANESE NICOLINO	PERSONALE (GESTIONE ECONOMICA) - TRIBUTI- CONTRIBUENTI - DIRITTO STUDIO - PROGRAMMAZIONE ECONOMICO FINANZIARIA
4+6	LUPINETTI BIAGIO	EDILIZIA - URBANISTICA - LLP VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI
Data di aggiornamento: 23/03/2011		

7.5 Incaricati dei trattamenti con il sistema informatico

Gli Incaricati del trattamento dei dati sono stati individuati dai Responsabili del trattamento ai sensi della deliberazione del Consiglio Comunale n. 2 del 26/01/2000 avente per oggetto: "Adozione del regolamento per il trattamento dei dati personali – L. 675/96 – D.LGS. 135/99".

Gli incaricati devono operare sotto la diretta autorità del Responsabile, attenendosi alle istruzioni impartite.

Il trattamento di dati personali con strumenti elettronici è consentito solo agli incaricati:

1) dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2) Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3) Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4) Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5) La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6) Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7) Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8) Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9) Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10) Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11) Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

12) Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13) I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14) Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Si riporta la tabella riepilogativa degli Incaricati preposti al trattamento dei dati personali con sistemi elettronici, contenente le seguenti informazioni:

1) *Identificativo Struttura trattamento:* contiene lo stesso identificativo utilizzato per identificare l'Archivio o Banca Dati.

2) *Incaricati del trattamento:* indica il nome degli incaricati del trattamento ai sensi dell'art. 30 del D.Lgs. 196/2003.

3) *Trattamenti operati dalla struttura:* indica i trattamenti per i quali la struttura ha la primaria responsabilità.

Tabella 2.3 Incaricati del trattamento di dati informatici

Identificativo Struttura Trattamento	Incaricati Trattamento	Trattamenti operati dagli Incaricati
1 + 2	1. LEONE ANTONIO	PERSONALE (STATO GIURIDICO)- ANAGRAFE - STATO CIVILE - ELETTORALE - COMMERCIO - SERVIZI SOCIALI
3	2. LANCIANESE NICOLINO	PERSONALE (GESTIONE ECONOMICA) - TRIBUTI- CONTRIBUENTI - DIRITTO STUDIO - PROGRAMMAZIONE ECONOMICO FINANZIARIA
4+6	3. LUPINETTI BIAGIO	EDILIZIA - URBANISTICA - LLP VERIFICHE URBANISTICO-EDILIZIE-AMBIENTALI
5	LEONE ANTONIO 4.DI DONATO ANTONIO	VIGILANZA STRADALE ALBO PRETORIO E POLIZIA AMMINISTRATIVA
Data di aggiornamento: 23/03/2011		

OPERATORI INCARICATI DELLA VERIFICA DEI PAGAMENTI SUPERIORI A 10.000 Euro

Con riferimento al DECRETO del MINISTERO DELL'ECONOMIA E DELLE FINANZE - 18 gennaio 2008, n. 40 Modalità di attuazione dell'articolo 48-bis del decreto del Presidente della Repubblica 29 settembre 1973, n. 602, recante disposizioni in materia di pagamenti da parte delle pubbliche amministrazioni viene applicata la seguente procedura.

Prima di effettuare il pagamento di un importo superiore a diecimila euro, si procede alla verifica inoltrando apposita richiesta a Equitalia Servizi S.p.A.

Viene comunicata ad Equitalia Servizi S.p.A. la documentazione contenente i dati anagrafici ed il codice fiscale dell'operatore incaricato di procedere al servizio di verifica, nonché l'indirizzo di posta elettronica cui ricevere le segnalazioni, al fine di consentire che quest'ultimo possa procedere alla propria registrazione.

Il trattamento dei dati è riservato esclusivamente agli operatori abilitati, quali soggetti incaricati ai sensi dell'articolo 30 del decreto legislativo 30 giugno 2003, n. 196.

Titolari del trattamento, ai sensi dell'articolo 28 del citato decreto legislativo sono i soggetti pubblici. Gli agenti della riscossione restano altresì titolari del trattamento dei dati inerenti agli inadempimenti. Responsabile del trattamento, ai sensi dell'articolo 29 dello stesso decreto legislativo n. 196 del 2003 è Equitalia Servizi S.p.A.

Il trattamento è ammesso esclusivamente per le finalità di cui all'articolo 48-bis comma 1, del decreto del Presidente della Repubblica n. 602 del 1973, secondo i principi di necessità, pertinenza e non eccedenza stabiliti dal decreto legislativo n. 196 del 2003.

Incaricati del trattamento di verifica di pagamenti superiori a 10.000,00 Euro

Identificativo Struttura Trattamento	Incaricati Trattamento	Trattamenti operati dagli Incaricati	Altre strutture Che concorrono al trattamento
3	LANCIANESE NICOLINO	Verifica dati personali per pgamenti superiori a 10.000 Euro	Equitalia Servizi SpA
Data di aggiornamento: 23/03/2011			

Note:

7.6 Analisi dei rischi che incombono sui dati trattati con il sistema informatico

L’analisi dei rischi ha permesso di individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati elettronici.

La relativa valutazione delle possibili conseguenze e il grado di gravità, così come sono state rilevate, impone l’adozione di adeguate misure di protezione.

Si riporta la tabella riepilogativa dell’analisi dei rischi, che incombono sul trattamento dei dati personali con sistemi elettronici, contenente le seguenti informazioni:

4) *Elenco degli eventi:* contiene l'elenco degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali.

5) *Impatto sulla sicurezza dei dati:* contiene la descrizione delle principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento ed una valutazione della gravità delle stesse, anche in relazione alla probabilità stimata dell'evento. L’indicatore di gravità è suddiviso su quattro livelli: alta/media/bassa/zero.

6) *Rif. misure d'azione:* contiene il riferimento alle contromisure adottata o programmate.

Tabella 3.1 - Archivi Elettronici: **Analisi dei rischi**

Evento		Impatto sulla sicurezza dei dati		Rif. misure d'azione (contromisure)
		Descrizione	Gravità stimata	
Comportamenti degli operatori	furto di credenziali di autenticazione	Furto di User e Password personali	alta	Custodia accurata di procedure di identificazione da parte di incaricati
	carenza di consapevolezza, disattenzione o incuria	Sottrazione o perdita dei dati	alta	Formazione, Note e circolari periodiche
	comportamenti sleali o fraudolenti	Uso improprio dei dati	media	Monitoraggio
	errori materiali	Dati errati e non corrispondenze	media	Processi di controllo e verifiche
Eventi relativi agli strumenti	azione di *virus* informatici o di codici malefici	Perdita dei dati	alta	Antivirus
	spamming o altre tecniche di sabotaggio	Blocco e ritardo operazioni	media	Firewall
	malfunzionamento, indisponibilità o degrado degli strumenti	Rallentamento operazioni, inefficienze	media	Controllo e adeguamento tecnologico di Hardware e periferiche
	accessi esterni non autorizzati	Sottrazione o indebita diffusione di dati	media	Porta con serratura
	intercettazione di informazioni in rete	Appropriazione di dati e utilizzo improprio o illecito	media	Scambio di dati su connessioni protette
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	Sottrazione o indebita diffusione di dati	alta	Controllo autorizzazioni e strumenti di identificazione
	asportazione e furto di strumenti contenenti dati	Perdita di dati	media	Dati localizzati su server e supporti, adeguata protezione dei relativi locali
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati	media	Conservazione dei dati su supporti conservati in diverso edificio o su server remoto
	guasto ai sistemi complementari (impianto elettrico, impianto di climatizzazione)	Perdita di dati	media	Salvavita, Gruppi di continuità collegati al Server e ai Clients, Condizionamento d'aria
	errori umani nella gestione della sicurezza fisica	Sottrazione o perdita dei dati	media	Distribuzione di compiti e funzioni di sicurezza incrociate
Data aggiornamento: 23/03/2011				

7.7 Misure in essere e da adottare per il trattamento dei dati con il sistema informatico

Nei locali del COMUNE DI CASTILENTI, ove avviene il trattamento dei dati personali in forma elettronica, è previsto un procedimento di controllo e di verifica della sicurezza del sistema informatico attraverso l'utilizzo di appositi strumenti a livello di sistema, di gestione delle basi dati e delle applicazioni.
Il sistema di controllo deve registrare gli accessi a livello di sistema, di base dati e di applicativo.

Ogni Responsabile del trattamento deve attribuire a uno o più incaricati, i quali operano sotto il suo controllo e nel rispetto delle sue direttive, il compito della verifica delle registrazioni. Il Responsabile risponde degli eventuali danni cagionati dagli incaricati, salvo che questi ultimi abbiano agito con dolo o colpa grave.

Le operazioni di verifica delle registrazioni devono essere effettuate con cadenza settimanale. I problemi comunque riscontrati devono essere prontamente riportati al responsabile del trattamento che individua le opportune contromisure.

CONTROLLO DEGLI ACCESSI

Tutte le stazioni di lavoro devono essere protette da una password di accesso.

L'inserimento della password di accesso va effettuato a cura dell'incaricato che ne deve affidare una copia in busta chiusa all'amministratore di sistema che le custodisce sotto chiave.

Ai fini dell'assistenza sistemistica, la password di accesso può venire comunicata agli operatori tecnici chiamati ad intervenire ed è sostituita al termine dell'intervento e mai più riutilizzata.

La password di accesso viene modificata al primo utilizzo e successivamente con cadenza trimestrale.

L'accesso alla rete di sistema deve essere protetto tramite un nome utente e una password.

Il processo di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo rispetto alle risorse del sistema informatico. A ciascun profilo viene associato un *gruppo* di utenti, che condivide gli stessi privilegi di accesso e utilizzo.

Il Responsabile del trattamento fornisce all'amministratore di sistema i nominativi e la qualifica degli utenti autorizzati, nonché i loro privilegi di utilizzo del sistema informatico.

L'amministratore di sistema provvede:

a. a definire, per ciascun utente, il nome utente e la password per il primo accesso;
b. a definire i gruppi necessari per rispettare i privilegi di utilizzo;

La password di accesso alla rete deve presentare sempre le seguenti caratteristiche:

a. non corrispondere al nome utente o ai dai dati personali dell'utente, né contenerne parti superiori ai due caratteri;
b. deve avere una lunghezza di almeno otto caratteri;
c. non deve corrisponde ad una parola di senso compiuto rintracciabile in un dizionario;
d. deve contenere almeno un carattere non alfabetico, oppure un misto di lettere minuscole e maiuscole;
e. non deve contenere riferimenti agevolmente riconducibili all'incaricato.

Il nome utente e la password sono strettamente personali; la loro tutela è a carico dell'utilizzatore.

L'amministratore di sistema, con cadenza trimestrale, provvede:

- alla verifica degli elenchi degli utenti
- alla disattivazione delle utenze su cui risultasse qualche problema, come il suo mancato utilizzo da più di sei mesi, o un elevato numero di tentativi di accesso non riusciti.

LE CONNESSIONI ALLA RETE LAN ED ALLA RETE INTERNET

Le connessioni telematiche verso le banche dati del server, devono essere consentite solo ai PC Client autorizzati e previa autenticazione.

Il collegamento verso l'esterno (rete internet) avviene a mezzo connessione ADSL per mezzo di un router. L'accesso dall'esterno è protetto a mezzo di un firewall informatico e si prevede di attivare un firewall fisico.

Il firewall è configurato in maniera tale da consentire alle postazioni di lavoro interne di accedere ai servizi disponibili sulla rete, bloccando i tentativi di accesso provenienti dall'esterno.

Non sono autorizzati collegamenti telematici diversi da quelli previsti ai punti precedenti. In particolare, non sono autorizzate connessioni effettuate tramite modem stand alone da postazioni collegate alla rete dell'ufficio.
Qualora siano necessarie connessioni di questo tipo, queste sono effettuate da PC non connessi alla rete LAN.

Utilizzo di Internet e della casella di posta elettronica istituzionale

In ottemperanza a:

- Il provvedimento del 1 marzo 2007del Garante per la protezione dei dati personali, riguardante il *Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori* ;
- La Direttiva n. 2 del 26 maggio 2009 del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri;

ai fini della predisposizione dei controlli sull'accesso e sul trattamento dei dati personali, si provvede ad approvare un **disciplinare** sulle attività consentite nell'**utilizzo di Internet e della casella di posta elettronica istituzionale** sul luogo di lavoro.

Il disciplinare ha per oggetto i criteri e le modalità operative di accesso e di utilizzo del servizio internet e di posta elettronica da parte dei dipendenti dell'ENTE e di tutti gli altri soggetti che, a vario titolo (lavoratori socialmente utili, collaboratori, tirocinanti, stagisti), operano nelle strutture dell'ENTE.

Albo pretorio: disposizioni a tutela dei dati personali pubblicati

La Legge 26.2.2010 n. 25 ha stabilito, come proroga finale, quella del 31 dicembre 2010, termine entro il quale la validità della pubblicità legale degli atti in forma cartacea, si accompagnava a quella elettronica.
Dal 1 gennaio 2011, quindi, è valida soltanto la pubblicazione degli atti sull'**Albo pretorio** tenuto sul sito internet dell'Ente.

In ottemperanza a quanto previsto:

- dall'art. 32 della legge n. 69/2009
- dagli articoli 18 e 19 del D.Lgs. 196/2003
- dalla Direttiva del Ministro per la pubblica amministrazione e l'innovazione 26 novembre 2009, n. 8

si prevede sul "**Regolamento per la disciplina delle attività di pubblicazione di atti, notizie e informazioni sul sito Istituzionale**" adottato tutte le misure atte a tutelare la riservatezza dei dati personali contenuti negli atti pubblicati.

In particolare, per quanto concerne il trattamento dei **dati sensibili e giudiziari**, esso è ammesso limitatamente alle modalità e procedure previste nel "Regolamento per il trattamento dei dati sensibili e giudiziari". La loro diffusione è consentita solo se strettamente indispensabile e prevista da espressa disposizione di legge o regolamento secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato. In tutti gli altri casi è espressamente vietata.

È in ogni caso espressamente vietato diffondere **dati idonei a rivelare lo stato di salute** degli interessati.

L'interessato deve essere **informato** del trattamento dei dati personali, con l'indicazione che gli stessi verranno diffusi tramite Internet sul sito del Comune e con le azioni che può esercitare a tutela del diritto alla riservatezza.

I dati personali pubblicati devono essere esatti, aggiornati, **pertinenti** e **non eccedenti** rispetto alle finalità. E' pertanto vietato diffondere atti eccedenti e non indispensabili a seconda dei casi, rispetto alle finalità perseguite (quali ad esempio: indirizzi, codici fiscali, coordinate bancarie, dati Ise e Isee). Analoga considerazione è formulata con riferimento ai dati personali la cui diffusione possa creare imbarazzo, disagio o esporre l'interessato a conseguenze indesiderate (indicazione di analitiche situazioni reddituali o particolari condizioni di bisogno o peculiari situazioni abitative), specie in riferimento a fasce deboli della popolazione (quali ad esempio: minori di età, anziani, soggetti o inseriti in programmi di recupero e di reinserimento sociale).
In questi casi particolari si rendono comunque applicabili le disposizioni previste dal "Regolamento recante norme per la semplificazione del procedimento per la disciplina degli albi dei beneficiari di provvidenze di natura economica, a norma dell'articolo 20, comma 8, della legge 15 marzo 1997, n. 59" *e* per le procedure concorsuali *e* le graduatorie dal "Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nel pubblici impieghi" che trova fondamento nella disposizione di cui all'art. 10 del D.Lgs. n. 267/2000.

La diffusione di dati personali attraverso il sito del comune comporta la conoscenza di dati da parte di un numero indeterminato di soggetti; per tale motivo per ogni attività di diffusione dei dati personali è necessaria una **valutazione preventiva** mirante ad accertare se le **finalità di**

trasparenza e di comunicazione possano essere perseguite senza divulgare tali dati, oppure valutando se sia possibile divulgare informazioni, atti e documenti con l'identificazione degli Interessati solo quando sia necessario.

Pur rispettando il principio di necessita è necessario verificare che i tipi di dati e il genere di operazioni svolte per pubblicarli e diffonderli siano **pertinenti** e **non eccedenti** rispetto alle finalità perseguite.

I dati devono essere formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione.

I dati personali pubblicati sul sito, una volta raggiunte le finalità per cui vengono pubblicati su internet, non devono più essere diffusi attraverso la prima pagina. A scopo di documentazione storica delle attività, e di mantenimento del patrimonio informativo comunale, anche le informazioni non più attuali vengono mantenute e rese accessibili in altre sezioni del sito garantendo il **diritto all'oblio**.

I contenuti dei file trasmessi per la pubblicazione devono essere attentamente analizzati da parte dei responsabili prima dell'invio per la pubblicazione sul sito. I Responsabili degli Uffici/Servizi/Aree devono verificare che l'eventuale presenza di dati personali nei documenti da pubblicare siano compatibili con le norme contenute nel D.Lgs 196/2003 e nella deliberazione del Garante per la protezione dei dati personali n. 17 del 19 aprile 2007 "linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali" e successive modifiche ed integrazioni.
È necessario adottare idonee misure preventive organizzative e tecnologiche per garantire la massima sicurezza dei dati e del patrimonio informativo presente sul sito istituzionale dell'Ente.
Gli atti nei quali sono contenuti dati personali non devono essere disponibili alla visione diretta mediante motori di ricerca esterni.
Nel rispetto di principi di sicurezza e inviolabilità dei dati pubblicati sul sito devono essere attuate le misure previste dagli articoli 31 e seguenti del D.Lgs. 196/2003 e dall'art. 51 del D.Lgs. 82/2005.
In particolare qualsiasi documento dovrà essere scaricabile dall'utente privato in un formato tale da impedire qualsiasi alterazione del medesimo, fatta eccezione unicamente per la modulistica per la quale si consente la compilazione in via informatica.

PROTEZIONE DELLE AREE E DEI LOCALI RILEVANTI AI FINI DELLA CUSTODIA DEI DATI OGGETTO DI TRATTAMENTO ELETTRONICO

Ai fini di evitare eventi dannosi o pericolosi ai dati oggetto di trattamento con strumenti elettronici il COMUNE DI CASTILENTI ha predisposto le seguenti misure di sicurezza:
Tutti i locali dove risiedono fisicamente le banche dati elettroniche vengono protetti con adeguate misure:

- Antintrusione, attraverso porte dotate di serratura e quelle che permettono l'accesso dall'esterno sono di tipo blindato, alle finestre esterne sono applicate grate metalliche;
- Antincendio, sono presenti estintori costantemente oggetto di manutenzione, sistemi antincendio con l'utilizzo di materiali ignifughi;
- Impianto di climatizzazione con condizionamento d'aria;
- Impianto elettrico è dotato di misure salvavita atte anche ed evitare cortocircuiti e possibili incendi e sono presenti gruppi di continuità collegati al Server e ai Clients per evitare danni ai dati personali trattati nell'ipotesi in cui venga a mancare l'erogazione della corrente elettrica.

Vengono di seguito riportate le tabelle riepilogative contenenti le seguenti informazioni sulle misure in essere e da adottare a contrasto dei rischi individuati dall'analisi dei rischi.

1) *Misure:* la descrizione sintetica della misura di sicurezza adottata.

2) *Rischio contrastato:* il riferimento all'elemento dell'analisi dei rischi che ha motivato l'adozione della misura in oggetto.

3) *Data base/trattamento interessato: data base* o archivio informatizzato dei trattamenti interessati per ciascuna delle misure adottate

4) *Rif. Scheda analitica:* eventuale riferimento ad una scheda analitica descrittiva della misura

5) *Data di effettività:* misura già operativa o data a partire dalla quale ne è prevista l'operatività

6) *Periodicità e modalità dei controlli:* periodicità con cui sono verificate la funzionalità e l'efficienza della misura e struttura operativa che ne ha la responsabilità.

Tab. 4.1 - Le misure di sicurezza adottate o da adottare

Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Rif. scheda Analitica (eventuale)	Misura già in essere	Misura da adottare	Periodicità e responsabilità dei controlli
Custodia accurata di procedure di identificazione da parte di incaricati	Furto di User e Password personali	Tutti	Tutte		SI		Trimestrale Responsabile Trattamento
Formazione, Note e circolari periodiche	Sottrazione o perdita dei dati per carenza di consapevolezza, disattenzione o incuria	Tutti	Tutte			Entro 2011	Rapportata a esigenze e innovazioni. Responsabile Trattamento
Monitoraggio	Uso improprio dei dati per comportamenti sleali o fraudolenti	Tutti	Tutte		SI		Responsabile Trattamento
Processi di controllo e verifiche	Dati errati e non corrispondenze per errori materiali	Tutti	Tutte		SI		Settimanale Responsabile Trattamento
Antivirus	Perdita dei dati per azione di *virus* informatici o di codici malefici	Tutti	Tutte		SI		Aggiornamento automatico Responsabile Trattamento
						Entro 2011	Amministratore sistema
Firewall informatico	Blocco e ritardo operazioni per *spamming* o altre tecniche di sabotaggio	Effettuati con PC connessi alla rete LAN	Aggiornate da PC connessi alla rete LAN		SI		Trimestrale Responsabile Trattamento
Firewall fisico					NO	Entro 2011	Amministratore sistema
Controllo e adeguamento tecnologico di Hardware e periferiche	Rallentamento operazioni, inefficienze per malfunzionamento, indisponibilità o degrado degli strumenti	Tutti	Tutte		SI		Trimestrale Responsabile Trattamento
						Entro 2011	Amministratore sistema
Porta con serratura	Sottrazione o indebita diffusione di dati per accessi esterni non autorizzati	Tutti	Tutte		SI		Mensile Responsabile Trattamento
Scambio di dati su connessioni protette	Appropriazione di dati e utilizzo improprio o illecito intercettazione di informazioni in rete	Effettuati con PC connessi alla rete LAN	Aggiornate da PC connessi alla rete LAN		SI		Trimestrale Responsabile Trattamento
						Entro 2011	Amministratore sistema

Segue Tab. 4.1

Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Rif. scheda Analitica (eventuale)	Misura già in essere	Misura da adottare	Periodicità e responsabilità dei controlli
Controllo autorizzazioni e strumenti di identificazione	Sottrazione o indebita diffusione di dati per accessi non autorizzati a locali/reparti ad accesso ristretto	Tutti	Tutte		SI		Quotidiano Responsabile Trattamento
Dati localizzati su server e supporti, adeguata protezione dei relativi locali	Perdita di dati per asportazione e furto di strumenti contenenti dati	Tutti	Tutte		SI		Quotidiano Titolare Trattamento
Conservazione dei dati su supporti conservati in diverso edificio o su server remoto	Perdita di dati per eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Tutti	Tutte		SI		Quotidiano Titolare Trattamento
Salvavita, gruppi di continuità collegati al Server e ai Clients	Perdita di dati per guasto ai sistemi complementari (impianto elettrico, climatizzazione)	Tutti	Tutte		SI		Mensile Titolare Trattamento
Condizionamento d'aria		Effettuati con PC connessi alla rete LAN	Aggiornate da PC connessi alla rete LAN		Entro 2011		
Distribuzione di compiti e funzioni di sicurezza incrociate	Sottrazione o perdita dei dati per errori umani nella gestione della sicurezza fisica	Tutti	Tutte		SI		Mensile Titolare Trattamento
Data aggiornamento: 23/03/2011							

PIANO DI VERIFICA PERIODICO DELLE MISURE ADOTTATE

L'efficacia delle misure adottate è periodicamente verificata secondo la seguente tabella:

Tab. 4.2 **Archivi elettronici**: Piano di verifica Misure di protezione

Attività	Verifiche	Periodicità	Riferimento normativo
Sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati.	Aggiornamento periodico a cadenza almeno annuale	Annuale	Allegato B al D. Lgs. n. 196/03
Individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici	Aggiornamento periodico a cadenza almeno annuale	Annuale	Allegato B al D. Lgs. n. 196/03
Misure contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale	Adozione di idonei strumenti, da eseguirsi con cadenza almeno Semestrale	Semestrale	Allegato B al D. Lgs. n. 196/03
Misure volte a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti	Aggiornamenti periodici, da eseguirsi con cadenza almeno trimestrale	Trimestrale	Allegato B al D. Lgs. n. 196/03
Controllo elenchi utenti	Verifica mancato utilizzo da più di sei mesi, o di elevato numero di tentativi di accesso non riusciti.	Trimestrale	Derivato Allegato B al D. Lgs. n. 196/03

7.8 Criteri e modalità per la conservazione e il ripristino della disponibilità dei dati elettronici

Le misure di sicurezza adottate, per quanto idonee a ridurre notevolmente gli eventuali episodi di danno o pericolo per i dati fatti oggetto di trattamento, non permettono, comunque, di escludere a priori che si possano verificare eventi eccezionali che comportino distruzione o danneggiamento degli stessi.

Per evitare che eventi dannosi si traducano nella perdita definitiva ed irrecuperabile dei dati trattati, tali informazioni sono protette attraverso:

- Copie di backup con cui si provvede a conservare la copia dei dati trattati elettronicamente;
- il supporto removibile è custodito in luogo sicuro, protetto e provvisto di impianto antincendio;
- vengono adottate misure di scurezza per i luoghi fisici in cui sono conservati i supporti mobili contenenti le copie di backup dei dati oggetto di trattamento.

Tab. 5.1 Conservazione dati elettronici

Salvataggio		Criteri individuati per il salvataggio (procedure operative in essere)	Ubicazione di conservazione delle copie	Struttura operativa incaricata del salvataggio
Data Base/Archivio	Dati sensibili o giudiziari contenuti			
1	Sensibili	Archivi elettronici su Server locale e su CD; Banche dati su unità di BackUp e Server remoto fornitore	Locali dell'Ufficio Finanziario in cassetti con serratura o in cassaforte e sul Server remoto del fornitore	Unità Operattiva Responsabile Trattamento
2	Sensibili + Giudiziari	Archivi elettronici su Server locale e su CD; Banche dati su unità di BackUp e Server remoto fornitore	Locali dell'Ufficio Finanziario in cassetti con serratura o in cassaforte e sul Server remoto del fornitore	Unità Operattiva Responsabile Trattamento
3	Comuni	Archivi elettronici su Server locale e su CD; Banche dati su unità di BackUp e Server remoto fornitore	Locali dell'Ufficio Finanziario in cassetti con serratura o in cassaforte e sul Server remoto del fornitore	Unità Operattiva Responsabile Trattamento
4	Giudiziari	Archivi elettronici su Server locale e su CD; Banche dati su unità di BackUp e Server remoto fornitore	Locali dell'Ufficio Finanziario in cassetti con serratura o in cassaforte e sul Server remoto del fornitore	Unità Operattiva Responsabile Trattamento
5	Giudiziari	Archivi elettronici su Server locale e su CD; Banche dati su unità di BackUp e Server remoto fornitore	Locali dell'Ufficio Finanziario in cassetti con serratura o in cassaforte e sul Server remoto del fornitore	Unità Operattiva Responsabile Trattamento
6	Giudiziari	Archivi elettronici su Server locale e su CD; Banche dati su unità di BackUp e Server remoto fornitore	Locali dell'Ufficio Finanziario in cassetti con serratura o in cassaforte e sul Server remoto del fornitore	Unità Operattiva Responsabile Trattamento
Data di aggiornamento: 23/03/2011				

Tab. 5.2. Ripristino dati elettronici

Rispristino		
Data base/archivio	Scheda operativa	Pianificazione delle prove di ripristino
1	Custodita dal Responsabile o suo Preposto	Trimestrale
2	Custodita dal Responsabile o suo Preposto	Trimestrale
3	Custodita dal Responsabile o suo Preposto	Trimestrale
4	Custodita dal Responsabile o suo Preposto	Trimestrale
5	Custodita dal Responsabile o suo Preposto	Trimestrale
6	Custodita dal Responsabile o suo Preposto	Trimestrale
Data aggiornamento: 23/03/2011		

7.9 Pianificazione degli interventi formativi previsti

Sono previsti interventi formativi degli incaricati del trattamento, per renderli edotti:

- dei 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 derivano dai compiti assegnati e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'assunzione dell'incarico, nonché:

- in occasione di cambiamenti di mansioni;
- di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- di mutamenti organizzativi o tecnologici delle misure adottate per la protezione dei dati personali;
- di modifiche e integrazioni della normativa in materia.

Viene di seguito riportata la tabella riepilogativa contenente le seguenti informazioni dell'impegno formativo che si prevede di sostenere in attuazione della normativa.

1) *Corso di formazione:* riporta l'identificativo del corso di formazione.

2) *Descrizione sintetica:* contiene la descrizione sintetica degli obiettivi del corso.

3) *Classi di incarico interessate:* contiene l'elenco delle classi omogenee di incarico a cui il corso è destinati e/o le tipologie di incaricati interessati.

4) *Numero di incaricati interessati:* contiene il numero di addetti interessati dal corso.

5) *Numero di incaricati già formati/da formare nell'anno:* contiene l'indicazione del numero di addetti già formati negli anni precedenti e quelli di cui si prevede la formazione nell'anno in corso.

Tab. 6.1 Pianificazione Corsi di Formazione

Corso di formazione	Descrizione sintetica Obiettivo	Classi di incarico interessate	Numero di incaricati interessati	Numero incaricati formati/da formare nell'anno	Calendario
1	Conoscenza delle norme in materia di Privacy e Sicurezza dei dati personali e dei provvedimenti giuridici del Garante per la loro corretta applicazione nella Pubblica Amministrazione.	Tutte	Tutti	Tutti da formare	Entro 2011
Data aggiornamento: 23/03/2011					

7.10 Trattamenti affidati all'esterno

Il Titolare del Trattamento dei dati o suo preposto deve richiedere:

- a tutti i fornitori di attrezzature informatiche e programmi utilizzati a livello comunale una dichiarazione scritta circa la compatibilità tecnologica dei relativi prodotti alle misure di sicurezza sopra descritte.
  Ove le caratteristiche tecnologiche di alcuni prodotti non risultassero pienamente soddisfacenti, i fornitori in questione dovranno indicare all'Azienda le soluzioni alternative realmente applicabili, dimostrandone la compatibilità con le misure minime di sicurezza riportate dall'Allegato B al D.Lgs. 30.06.2003 n. 196 contenente il disciplinare tecnico in materia di misure minime di sicurezza.

- a tutti i fornitori delle attività trasferite a terzi che comportano il trattamento di dati personali una dichiarazione scritta circa il rispetto delle misure minime di sicurezza, riportate dall'Allegato B al D.Lgs. 30.06.2003 n. 196, con l'indicazione sintetica del quadro contrattuale in cui tale trasferimento si inserisce, in riferimento alla protezione dei dati personali.

In particolare il soggetto cui le attività sono affidate dichiara:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;

2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;

3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;

4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze;

5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Viene di seguito riportata la tabella riepilogativa contenente le seguenti informazioni dei trattamenti affidati all'esterno.

1) *Attività delegata:* contiene l'identificativo dell'attività che è stata oggetto di delega a terzi.

2) *Descrizione sintetica:* contiene una descrizione sintetica dell'attività.

3) *Dati personali, sensibili o giudiziari interessati:* contiene l'elenco dei dati personali, sensibili o giudiziari oggetto di trattamento per la realizzazione dell'attività delegata.

4) *Soggetto delegato:* riporta l'identificativo della società o del consulente a cui è stato affidato l'incarico.

5) *Descrizione dei criteri per garantire l'adozione delle misure:* perché sia garantito un adeguato trattamento dei dati è necessario che il soggetto esterno a cui viene affidato il trattamento si assuma alcuni impegni su base contrattuale.

Tab. 7.1 Archivi elettronici**: Trattamenti affidati all'esterno**

Attività esternalizzata	Descrizione sintetica	Dati personali, sensibili o giudiziari interessati	Soggetto esterno	Descrizione dei criteri per l'adozione delle misure
GESTIONE SISTEMA INFORMATIVO	ATTIVITÀ DI RISCOSSIONE TASSE E IMPOSTE COMUNALI	giudiziari	HALLEY	Misure riservate ai fornitori delle attività trasferite a terzi che comportano il trattamento di dati personali
TRIBUTI	ATTIVITÀ DI RISCOSSIONE TASSE E IMPOSTE COMUNALI	comuni	CONCESSIONARIO	Misure riservate ai fornitori delle attività trasferite a terzi che comportano il trattamento di dati personali
CITTADINI	CONTRIBUTI A CITTADINI SVANTAGGIATI	sensibili	INPS	TRASMISSIONE TELEMATICA IN AMBIENTE PROTETTO
DIPENDENTI	CONTRIBUTI SOCIO ASSISTENZIALI	sensibili	INPS – INPDAP - INAIL	TRASMISSIONE TELEMATICA IN AMBIENTE PROTETTO
DIPENDENTI	CONTRIBUTI FISCALI	comuni	AGENZIA DELLE ENTRATE	TRASMISSIONE TELEMATICA IN AMBIENTE PROTETTO
DIPENDENTI	SICUREZZA SUL LOVORO	comuni	PEGASO S.R.L. MONTORIO V.	Misure riservate ai fornitori delle attività trasferite a terzi che comportano il trattamento di dati personali
CITTADINI	CONTRIBUTI A CITTADINI SVANTAGGIATI BONUS ENERGIA ELETTRICA	sensibili	SGATE	TRASMISSIONE TELEMATICA IN AMBIENTE PROTETTO
CITTADINI	CONTRIBUTI A CITTADINI SVANTAGGIATI BONUS ENERGIA GAS	comuni	SGATE	TRASMISSIONE TELEMATICA IN AMBIENTE PROTETTO
Data di aggiornamento: 23/03/2011				

8. DICHIARAZIONE D'IMPEGNO E FIRMA

Il presente documento, redatto in data _____, viene firmato in calce dal Sindaco o dal Commissario Straordinario in qualità di Titolare *pro-tempore*, e verrà aggiornato periodicamente entro il 31 marzo di ogni anno.

L'originale del presente documento è custodito presso la sede della società, per essere esibito in caso di controllo.

Una copia verrà consegnata ai Responsabili del trattamento dei dati appositamente nominati.

Castilenti, li _____

Firma Titolare del Trattamento

_____

ALLEGATO 1

INFORMAZIONI SULLA PROTEZIONE DEI DATI PERSONALI
come previsto dal decreto legislativo 30 giugno 2003, n. 196
"Codice in materia di protezione dei dati personali"

Di seguito riportiamo alcune informazioni utili per chi fornisce al Comune di Castilenti (TE) i propri dati personali tramite la compilazione dei moduli:

- l'indicazione nel modulo dei propri dati personali è obbligatoria, altrimenti la richiesta non può essere presa in considerazione;

- il Comune di Castilenti usa i dati personali contenuti nel modulo per soddisfare la relativa richiesta, e li elabora con data base informatici o cartacei. Se un servizio è svolto da un soggetto terzo (azienda privata, azienda pubblica, ecc.) per conto dell'Ente, i dati possono essere forniti anche a questo soggetto;

- in ogni momento è possibile chiedere al Comune informazioni sui propri dati personali , e chiederne la rettifica, l'integrazione o la cancellazione.
A tal fine, sul modulo sono indicati il Responsabile del procedimento e del trattamento dei dati a cui rivolgersi, oltre al servizio che si occuperà della richiesta e la direzione cui lo stesso fa capo;

- per conoscere tutti i diritti è possibile leggere l'articolo 7 del decreto legislativo n. 196 del 2003 "codice in materia di protezione dei dati personali", sotto riportato;

- L'elenco completo di tutti i Responsabili del trattamento dei dati del Comune di Castilenti è disponibile al link "responsabili privacy".

Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del Titolare, e dei responsabili del trattamento dei dati personali;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Per consultare il testo completo del decreto legislativo n. 196 del 2003 "codice in materia di protezione dei dati personali", visita il sito del Garante per la protezione dei dati personali.

Comune di Castilenti ____/____/_____

ALLEGATO 2

NOMINA RESPONSABILE TRATTAMENTO DEI DATI PERSONALI

Quale titolare del trattamento dei dati personali ai sensi dell'art. 28 del dlgs 196/03, Vi nominiamo responsabile del trattamento ai sensi dell'art. 29 del provvedimento citato, in quanto ha fornito garanzia di esperienza, capacità e affidabilità come richiesto dalla normativa vigente, limitatamente all'Ufficio ……

Con la sottoscrizione della presente accetta la nomina e si impegna a procedere al trattamento dei dati personali attenendosi alle istruzioni impartite nel pieno rispetto di quanto imposto dall'art. 29, comma 5, dal predetto decreto legislativo, dichiarandosi altresì edotto degli obblighi previsti a carico del Responsabile.

Quale responsabile si impegna nel tempo tecnicamente necessario eventualmente ad impartire per iscritto agli incaricati e istruzioni relative al trattamento e a verificare la loro applicazione, in conformità a quanto previsto dall'Allegato B al decreto stesso.

Quale responsabile si impegna inoltre ad adottare o a far adottare le misure di sicurezza prescritte da atti regolamentari o comunque necessarie secondo le norme di buona tecnica.

Per l'espletamento dell'incarico Le vengono assegnati i necessari poteri e supporti organizzativi.

Ai sensi dell'art. 29 citato, Lei dichiara di aver ricevuto, esaminato e compreso le istruzioni sul trattamento riportate qui di seguito, dichiarandosi disponibile e competente per la piena attuazione di quanto ivi disposto:

- catalogare analiticamente le banche dati con tutti gli elementi necessari anche ai fini della loro eventuale notifica al Garante;
- individuare gli incaricati del trattamento e impartire loro per iscritto le istruzioni ed autorizzazioni necessarie ad un corretto, lecito e sicuro trattamento e verificarne la puntuale applicazione
- attuare gli obblighi di informazione ad acquisizione del consenso, quando richiesto, nei confronti degli interessati
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dagli artt. 7 e segg. dlgs. 196/03
- predisporre la eventuale notificazione iniziale al Garante delle banche dati e delle successive eventuali modifiche che le dovessero riguardare, verificando l'esattezza e la completezza dei dati contenuti, salve restando le esclusioni dell'obbligo di notifica previste dalla legge;
- collaborare per l'attuazione delle prescrizioni impartite dal Garante;
- predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni degli artt. 33/36 e dell'allegato B del DLGS 196/03, nonché adeguare il sistema alle norme regolamentari in materia di sicurezza

Si impegna a comunicare al titolare qualsiasi variazione della situazione oggettiva o soggettiva, tali da compromettere il corretto espletamento dei compiti prescritti.

Nell'adempimento dell'incarico agirà con piena autonomia.

_____, lì _____ _____

(firma Titolare del Trattamento)

Il sottoscritto …….....dichiara di accettare l'incarico sopra conferito.

Castilenti, li _____ _____

(*firma)*

ALLEGATO 3

NOMINA INCARICATO TRATTAMENTO DEI DATI PERSONALI

Visto il decreto legislativo 196/03 Le precisiamo quanto segue.

1) La nominiamo incaricato del trattamento dei dati personali utilizzati nell'ambito dell'attività lavorativa prestata nella nostra struttura.
Pertanto nello svolgimento delle Sue mansioni potrà eseguire il trattamento dei dati personali ai quali ha accesso ed inerenti al Suo Ufficio, compresa la comunicazione degli stessi.
Il trattamento avverrà sia con sistemi cartacei che meccanizzati e potrà comprendere tutte le operazioni di cui al punto a) dell'art. 4 del decreto legislativo 196/03.
Il trattamento dei dati verrà compiuto esclusivamente nell'ambito delle mansioni a Lei affidate e precisamente:

……

Dovrà essere attuato in modo da evitare accessi non autorizzati o diffusione di dati, compiendo le operazioni strettamente necessarie alla Sua mansione .

2) In particolare le operazioni di trattamento consentito sono le seguenti:
……

3) Nell'ambito delle mansioni svolte potrà trattare i seguenti dati:
……..…..

4) Gli strumenti che potrà usare per il trattamento dei dati sono i seguenti:
……..…..

Potrà inoltre accedere agli archivi cartacei riguardanti …….

5) Le precisiamo che per l'accesso ai dati personali e agli archivi a cui è demandata la Sua attività dovrà utilizzare un codice di identificazione attribuitole in maniera riservata nonché una parola chiave da Lei predisposta composta di almeno otto caratteri. Tale parola chiave dovrà essere da Lei sostituita ogni volta che verrà fatta espressa richiesta in tal senso da parte del titolare o del responsabile del trattamento e comunque almeno ogni sei mesi (almeno ogni tre mesi se vengono da Lei trattati anche dati sensibili o giudiziari)

6) Le ricordiamo che il codice di identificazione, se utilizzato, così come la sua parola chiave, sono strettamente personali e non possono essere utilizzati da altri.

7) I sistemi di autorizzazione, quali la parola chiave o simili, diverse da quelle autorizzate per soli scopi di gestione tecnica, verranno disattivate automaticamente qualora non utilizzati da almeno sei mesi.
Ugualmente i sistemi saranno disattivati in caso di perdita della qualità o della mansione, che Le consente l'accesso ai dati personali di cui sopra, in tutto o in parte.

8) Rammentiamo che per ogni sessione di lavoro dovrà curare che il Suo strumento informatico non rimanga incustodito o accessibile ad altri in Sua assenza; in particolare in caso di assenza dovrà assicurarsi che la Sua postazione risulti protetta verificando le protezioni relative.
Inoltre dovranno essere seguite le seguenti indicazioni:
…….

9) La parola chiave prescelta ed ogni variazione della stessa dovrà venire comunicata immediatamente al preposto alla custodia delle parole chiave, il cui nominativo è Sig. ……. mediante apposita nota contenente il Suo nome e cognome, l'elaboratore utilizzato, la parola chiave e la decorrenza della stessa.
La mancata comunicazione potrà costituire comportamento illecito disciplinare, come tale sanzionabile ai sensi di legge e di contratto.

10) In caso di utilizzo di supporti rimovibili per la memorizzazione dei dati dovranno essere rispettate le seguenti istruzioni: *chiusura in armadi; utilizzo soltanto da parte degli incaricati nominati; divieto di copie non autorizzate.*

11) E' autorizzato ad effettuare operazioni di trattamento relativamente ai dati sensibili (art. 26 decreto legislativo 196/03) riguardanti le seguenti banche dati: ……. La predetta autorizzazione è limitata ai dati necessari allo svolgimento della attività e della Sua mansione e precisamente …….
I supporti rimovibili non utilizzati vanno distrutti o resi inutilizzabili ovvero i dati vanno resi inintelligibili se non usati da altri incaricati autorizzati.

12) In caso di trattamento di dati con sistemi non automatizzati (cartacei) avrà accesso soltanto ai dati la cui conoscenza è necessaria al compimento dell'attività e delle mansioni a Lei affidate ed in particolare ai seguenti documenti e dati:
……..
……..

13) Sempre in caso di trattamento di dati con sistemi non automatizzati (cartacei) gli atti e i documenti dati sensibili ai sensi dell'art. 26 Dlgs. 196/03 dovranno venire da Lei conservati in modo da evitare intrusioni o accessi non autorizzati e restituiti al responsabile.
Tali cautele dovranno altresì essere osservate in caso di riproduzione su documenti cartacei o simili di informazioni relative al trattamento di dati sensibili.

14) Ancora in riferimento ai dati trattati senza l'ausilio di strumenti elettronici dovranno comunque essere rispettate le seguenti istruzioni: *chiusura in armadi; utilizzo soltanto da parte degli incaricati nominati; divieto di copie non autorizzate.*

Castilenti, li _____

Il Responsabile del trattamento

_____

L'Incaricato

_____

ALLEGATO 4

INFORMATIVA PRIVACY (Art.13 del D.lgs.30 giugno 2003 n. 196)

per MODULISTICA COMUNALE

Ai sensi dell'art.13 del Codice in materia di dati personali si informa che il trattamento dei dati personali forniti per _____ è finalizzato unicamente alla corretta esecuzione dei compiti istituzionali nelle singole materie che disciplinano i servizi ed avverrà presso il Comune di Castilenti, Via _____ n. ____ con l'utilizzo di procedure anche informatizzate, nei modi e nei limiti necessari per perseguire le predette finalità. I dati potranno essere comunicati o portati a conoscenza di responsabili ed incaricati di altri soggetti pubblici che debbano partecipare al procedimento amministrativo. I dati potranno altresì essere comunicati o portati a conoscenza dei seguenti responsabili o incaricati del trattamento: Incaricati e responsabili del trattamento dati impiegati presso il servizio protocollo e archivio e incaricati e responsabili del trattamento dati impiegati presso i singoli servizi comunali interessati dalla richiesta. Il conferimento dei dati è obbligatorio per poter concludere positivamente il procedimento amministrativo e la loro mancata indicazione comporta quindi l'impossibilità di beneficiare del servizio ovvero della prestazione finale. Agli interessati sono riconosciuti i diritti di cui all'art.7 del citato codice ed in particolare il diritto di accedere ai propri dati personali, di chiederne la rettifica, l'aggiornamento e la cancellazione, se incompleti, erronei o raccolti in violazione della legge, nonché di opporsi al loro trattamento per motivi legittimi, rivolgendo le richieste al Titolare del trattamento: Comune di Castilenti (TE), Via _____, _____ Castilenti. Il Responsabile del trattamento per il Servizio _____ è il Sig. _____, Via _____(domicilio comunale)_____, _____ Castilenti (TE) .

ALLEGATO 5

POLICY PRIVACY SITO WEB

In questa pagina si descrivono le modalità di gestione del sito in riferimento al trattamento dei dati personali degli utenti che lo consultano.

Si tratta di un'informativa che è resa anche ai sensi dell'art. 13 del d.lgs. n. 196/2003 - Codice in materia di protezione dei dati personali a coloro che interagiscono con i servizi *web* resi accessibili per via telematica a partire dall'indirizzo:

http://www_____

corrispondente alla pagina iniziale del sito "_____".

L'informativa è resa solo per il sito _____ e non anche per altri siti *web* eventualmente consultati dall'utente tramite *link*.

L'informativa si ispira anche alla Raccomandazione n. 2/2001 che le autorità europee per la protezione dei dati personali, riunite nel Gruppo istituito dall'art. 29 della direttiva n. 95/46/CE , hanno adottato il 17 maggio 2001 per individuare alcuni requisiti minimi per la raccolta di dati personali *on-line*, e, in particolare, le modalità, i tempi e la natura delle informazioni che i titolari del trattamento devono fornire agli utenti quando questi si collegano a pagine *web*, indipendentemente dagli scopi del collegamento.

IL "TITOLARE" DEL TRATTAMENTO

A seguito della consultazione di questo sito possono essere trattati dati relativi a persone identificate o identificabili.

Il "titolare" del loro trattamento è
il _____.

LUOGO DI TRATTAMENTO DEI DATI

I trattamenti connessi ai servizi *web* di questo sito hanno luogo presso la predetta sede del Titolare e sono curati solo da personale tecnico dell'Ufficio incaricato del trattamento, oppure da eventuali incaricati di occasionali operazioni di manutenzione.

Nessun dato derivante dal servizio *web* viene comunicato o diffuso.

I dati personali forniti dagli utenti che inoltrano richieste di invio di materiale informativo, risposte a quesiti, offerte di prestazioni e prodotti, sono utilizzati al solo fine di eseguire il servizio o la prestazione richiesta e sono comunicati a terzi nel solo caso in cui ciò sia a tal fine necessario.

TIPI DI DATI TRATTATI

Dati di navigazione

I sistemi informatici e le procedure *software* preposte al funzionamento di questo sito *web* acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione *URI (Uniform Resource Identifier)* delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal *server* (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del sito e per controllarne il corretto funzionamento e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del sito: salva questa eventualità, allo stato i dati sui contatti *web* non persistono per più di sette giorni.

Dati forniti volontariamente dall'utente

L'invio facoltativo, esplicito e volontario di posta elettronica agli indirizzi indicati su questo sito comporta la successiva acquisizione dell'indirizzo del mittente, necessario per rispondere alle richieste, nonché degli eventuali altri dati personali inseriti nella missiva.

Specifiche informative di sintesi verranno progressivamente riportate o visualizzate nelle pagine del sito predisposte per particolari servizi a richiesta.

COOKIES

Nessun dato personale degli utenti viene in proposito acquisito dal sito.

Non viene fatto uso di *cookies* per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. *cookies* persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

L'uso di c.d. *cookies* di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal *server*) necessari per consentire l'esplorazione sicura ed efficiente del sito.

I c.d. *cookies* di sessione utilizzati in questo sito evitano il ricorso ad altre tecniche informatiche

potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

FACOLTATIVITA' DEL CONFERIMENTO DEI DATI

A parte quanto specificato per i dati di navigazione, l'utente è libero di fornire i dati personali riportati nei moduli di richiesta a _____ o comunque indicati in contatti con l'Ufficio per sollecitare l'invio di materiale informativo o di altre comunicazioni.

Il loro mancato conferimento può comportare l'impossibilità di ottenere quanto richiesto.

MODALITA' DEL TRATTAMENTO

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

DIRITTI DEGLI INTERESSATI

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (art. 7 del d.lgs. n. 196/2003).

Ai sensi del medesimo articolo si ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Le richieste vanno rivolte al titolare del trattamento

P3P

La presente informativa sulla *privacy* è consultabile in forma automatica dai più recenti *browser* che implementano lo *standard* P3P ("*Platform for Privacy Preferences Project*") proposto dal *World Wide Web Consortium* (www.w3c.org).

Ogni sforzo verrà fatto per rendere il più possibile interoperabili le funzionalità di questo sito con i meccanismi di controllo automatico della *privacy* disponibili in alcuni prodotti utilizzati dagli utenti.

Considerando che lo stato di perfezionamento dei meccanismi automatici di controllo non li rende attualmente esenti da errori e disfunzioni, si precisa che il presente documento, pubblicato all'indirizzo

http://www._____ ,

costituisce la "*Privacy Policy*" di questo sito che sarà soggetta ad aggiornamenti.

ALLEGATO 6

NOMINA DELL'AMMINISTRATORE DI SISTEMA

Spett. . ……...……

Oggetto: Nomina ad "Amministratore del sistema informativo"

Considerando che per preparazione ed esperienza la sua società/Lei fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nella custodia e nel trattamento dei dati personali, con la presente Le conferiamo il compito di sovrintendere alle risorse del sistema informativo del Comune di Castilenti e di consentirne l'utilizzazione.

In tale contesto sarà Suo compito:

- individuare per iscritto il/i soggetto/i incaricato/i della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla sua attività;
- individuare per iscritto gli altri soggetti, diversi dal/dagli incaricato/i della custodia delle parole chiave, che possono avere accesso ad informazioni che concernono le medesime;
- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 1 a 10 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dai punti da 12 a 14 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- verificare costantemente che il nostro Ente abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dall'art. 34 del D. Lgs. n. 196/2003, e dal Disciplinare tecnico, allegato B) al decreto legislativo medesimo, provvedendo senza indugio agli adeguamenti eventualmente necessari;
- proporre al Titolare o al Responsabile dello specifico trattamento, se nominato, l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a realizzare quanto previsto dall'art. 31 del D. Lgs. n. 196/2003, che dispone che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da 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;
- curare, su incarico del Titolare del trattamento, l'adozione e l'aggiornamento delle misure "idonee" di cui al punto precedente;

- attivare e aggiornare con cadenza almeno trimestrale idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo a Lei affidato, contro il rischio di intrusione e contro l'azione dei virus informatici;
- aggiornare periodicamente, con frequenza almeno annuale (*oppure* semestrale *se si trattano dati sensibili o giudiziari*), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- redigere schede procedurali ed impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, dell'efficacia delle misure di sicurezza adottate in azienda.

Sarà Suo compito riferire periodicamente, ed in ogni caso con cadenza trimestrale, al Titolare sullo svolgimento dei Suoi compiti, dandogli inoltre piena collaborazione nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.

Al fine di una migliore comprensione dei Suoi compiti specifici relativi alla corretta e sicura gestione del sistema informativo aziendale, alleghiamo alla presente il Documento Programmatico sulla Sicurezza redatto ai sensi del D. Lgs. n. 196/2003, e del Disciplinare tecnico, allegato B) al decreto legislativo medesimo.
La preghiamo di restituirci copia della presente, firmata per accettazione e per ricevuta della documentazione di cui sopra.
Distinti saluti.

Data, _____

_____
Firma Titolare del trattamento

Per ricevuta ed accettazione _____
(data e firma)

ALLEGATO 7

RICHIESTA A FORNITORE DI ATTIVITÀ ESTERNE
DELLA DICHIARAZIONE DI RISPETTO DELLE MISURE MINIME DI SICUREZZA

(Allegato B del DLGS. 196/03)

L'Allegato B del D.Lgs. 30.06.2003 n. 196, sulle misure di sicurezza relative alla tutela dei dati personali prevede l'obbligo di richiedere a tutti i fornitori di attività trasferite a terzi e svolte all'esterno dei locali comunali, che comportano il trattamento di dati personali, una dichiarazione scritta circa il rispetto delle misure minime di sicurezza.

Come previsto anche dal "Documento Programmatico sulla Sicurezza per la protezione dei dati personali in materia di misure minime di sicurezza", adottato da questo Comune con la Deliberazione di Giunta Comunale n. _____ del ____/____/_____ vogliate, rimetterci la Vostra Dichiarazione scritta circa:

1. la consapevolezza che i dati da Voi trattati, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione del Codice per la protezione dei dati personali;

2. l'ottemperanza agli obblighi previsti dal Codice per la protezione dei dati personali;

3. l'adozione delle istruzioni specifiche ricevute, in qualità di incaricato, per il trattamento dei dati personali e la relativa integrazione nelle procedure già in essere;

4. l'impegno a relazionare annualmente sulle misure di sicurezza adottate e ad allertare immediatamente il Comune di Castilenti, in qualità di committente, in caso di situazioni anomale o di emergenze;

5. il riconoscimento, al Comune di Castilenti, del diritto a verificare periodicamente l'applicazione delle norme di sicurezza da Voi adottate.

La Dichiarazione di cui sopra ci dovrà essere rimessa entro 10 (dieci) giorni dal ricevimento della presente.

Distinti saluti.

_____, lì

_____

Il Responsabile del trattamento

ALLEGATO 8

RICHIESTA A FORNITORE DI ATTIVITÀ INTERNE DELLA DICHIARAZIONE DI RISPETTO DELLE MISURE MINIME DI SICUREZZA

(Allegato B del DLGS. 196/03)

L'Allegato B del D.Lgs. 30.06.2003 n. 196, sulle misure di sicurezza relative alla tutela dei dati personali prevede l'obbligo di richiedere a tutti i fornitori di attività trasferite a terzi e svolte all'interno dei locali comunali, che comportano il trattamento di dati personali, una dichiarazione scritta circa il rispetto delle misure minime di sicurezza.

Come previsto anche dal "Documento Programmatico sulla Sicurezza per la protezione dei dati personali in materia di misure minime di sicurezza", adottato da questo Comune con la Deliberazione di Giunta Comunale n. _____ del ____/____/_____, vogliate rimetterci la Vostra Dichiarazione scritta circa:

1. la consapevolezza che i dati da Voi trattati, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del Codice per la protezione dei dati personali;

2. l'ottemperanza agli obblighi previsti dal Codice per la protezione dei dati personali;

3. l'adozione delle istruzioni specifiche ricevute, in qualità di incaricato, per il trattamento dei dati personali e la integrazione nelle procedure già in essere;

4. l'impegno a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il Comune di Castilenti, in qualità di committente, in caso di situazioni anomale o di emergenze;

5. di riconoscere il diritto del Comune di Castilenti a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

La Dichiarazione di cui sopra ci dovrà essere rimessa entro 10 (dieci) giorni dal ricevimento della presente.

Vogliate, inoltre, cortesemente fornirci i nominativi delle persone che la Vostra Ditta ha assegnato alle attività in oggetto nei nostri locali situati in _____ e ciò anche al fine di poter considerare tali persone autorizzate all'accesso nei nostri locali.

In caso di assenza o impedimento delle persone che ci indicherete, sarà Vostra cura, ed obbligo, comunicarci i nominativi dei sostituti.

Ai fini dei controlli e delle responsabilità civili e penali connessi alla violazione delle norme contenute nel decreto, Vi informiamo di aver predisposto un Registro delle persone autorizzate ad accedere ai nostri locali (oppure: sarà opportuno che la Vostra Ditta organizzi un registro delle persone autorizzate ad accedere nei nostri locali), da cui dovrà risultarne la presenza.

Distinti saluti.

_____, li_____

_____

Il Responsabile del trattamento

ALLEGATO 9

RICHIESTA A FORNITORI DELLA DICHIARAZIONE DI COMPATIBILITÀ TECNOLOGICA DELLE ATTREZZATURE E PROGRAMMI INFORMATICI ALLE MISURE MINIME DI SICUREZZA

(Allegato B del DLGS. 196/03)

L'Allegato B del D.Lgs. 30.06.2003 n. 196, sulle misure di sicurezza relative alla tutela dei dati personali prevede l'obbligo di richiedere a tutti i fornitori di attrezzature e programmi informatici utilizzati a livello comunale una dichiarazione scritta circa il rispetto delle misure minime di sicurezza.

Come previsto anche dal "Documento Programmatico sulla Sicurezza per la protezione dei dati personali in materia di misure minime di sicurezza" adottato da questo Comune con la Deliberazione di Giunta Comunale n. _____ del ____/____/_____, vogliate rimetterci la Vostra Dichiarazione scritta circa:

- la compatibilità tecnologica delle attrezzature informatiche, programmi e altri prodotti da Voi fornitici alle misure di sicurezza previste dall'Allegato B del DLGS. 196/03.

La Dichiarazione in oggetto ci dovrà essere rimessa:

- entro 10 (dieci) giorni dal ricevimento della presente per le forniture già effettuate;
- in futuro ogni qualvolta provvederete ad eventuali ulteriori forniture nei nostri confronti.

Ove le caratteristiche tecnologiche di alcuni prodotti non risultassero pienamente soddisfacenti, vogliate indicarci le soluzioni alternative realmente applicabili, dimostrandone la compatibilità con le misure minime di sicurezza riportate dall'Allegato B al D.Lgs. 30.06.2003 n. 196.

Distinti saluti.

_____, li _____

_____

Il Responsabile del trattamento

ALLEGATO 10

AUTORIZZAZIONE PER L'ACCESSO AI LOCALI DEI SOGGETTI AMMESSI AGLI ARCHIVI DOPO L'ORARIO DI CHIUSURA

In relazione agli obblighi di cui all'Allegato B del DLGS. 196/03 sulle misure di sicurezza relative alla tutela dei dati personali è previsto anche quello - in determinate circostanze - della **"identificazione e registrazione dei soggetti ammessi agli archivi dopo l'orario di chiusura"**. Infatti, la protezione degli archivi è estesa alla custodia e conservazione di ogni atto e documento cartaceo contenente dati personali sensibili e giudiziari.

Allo scopo, in ottemperanza alle suddette necessità di legge, vogliate cortesemente fornirci i nominativi delle persone che la Vostra ditta ha assegnato alle pulizie dei nostri locali situati in _____ e ciò anche al fine di poter considerare tali persone autorizzate all'accesso nei nostri locali. In caso di assenza o impedimento delle persone che ci indicherete, sarà Vostra cura, ed obbligo, comunicarci i nominativi dei sostituti.

Ai fini dei controlli e delle responsabilità civili e penali connessi alla violazione delle norme contenute nel decreto sarà opportuno che la Vostra ditta organizzi un registro delle persone autorizzate ad accedere nei nostri locali (*oppure*: Vi informiamo di aver predisposto un registro delle persone autorizzate ad accedere ai nostri locali), da cui dovrà risultare la presenza.

Le persone autorizzate dovranno limitarsi alle sole attività di pulizia. Il materiale cartaceo asportato destinato allo smaltimento dei rifiuti, dovrà essere riposto con cura negli appositi sacchi di plastica e, tali sacchi dovranno essere chiusi in maniera che gli atti e i documenti in essi contenuti non possano, nemmeno accidentalmente, fuoriuscire.

Tale condotta dovrà essere rispettata dal Vostro personale che, allo scopo, sarà da Voi informato.

Distinti saluti.

_____, li _____

_____

Il Titolare o il Responsabile del trattamento

ALLEGATO 11

CARTELLO PER VIDEOSORVEGLIANZA

IL PRESENTE LOCALE PER RAGIONI DI SICUREZZA E' SORVEGLIATO DA SISTEMA DI VIDEOSORVEGLIANZA FISSA A MEZZO _____.

LE IMMAGINI VENGONO REGISTRATE E CONSERVATE NEL SEGUENTE MODO: _____

(*oppure se non registrate*:
LE IMMAGINI VENGONO RILEVATE NEL SEGUENTE MODO: _____)

(*se registrate*) LE IMMAGINI SONO CONSERVATE PER GIORNI _____ CON IL SEGUENTE SISTEMA:_____, SALVE ESIGENZE DI GIUSTIZIA.

L'USO DEI SISTEMI E IL TRATTAMENTO DELLE IMMAGINI E' DEMANDATO ESCLUSIVAMENTE AI SOGGETTI SPECIFICAMENTE INCARICATI.

IL CONFERIMENTO DEI DATI (IMMAGINI) NON E' OBBLIGATORIO, MA IL DIVIETO DI RIPRESA POTRA' COMPORTARE L'IMPOSSIBILITA' DI AUTORIZZARE L'ACCESSO AI LUOGHI OGGETTO DI VIDEOSORVEGLIANZA.
RESTANO FERME LE ESIGENZE DI CONTROLLO E SICUREZZA ANCHE NELL'AMBITO DI INDAGINI INVESTIGATIVE.

I SOGGETTI INTERESSATI RIPRESI DALLE VIDEOCAMERE POSSONO ESERCITARE I DIRITTI DI CUI ALL'ART. 7 DEL DECRETO LEGISLATIVO N. 196/2003.

RESPONSABILE DEL TRATTAMENTO DEI DATI E' _____

(*se nominato);*

(oppure:

TITOLARE DEL TRATTAMENTO DEI DATI E'_____).