Città di Segrate

Provvedimento n. 97

Segrate, DA 5 AGO 2010

OGGETTO: **Adozione del "Documento Programmatico sulla Sicurezza" ai sensi del Decreto Legislativo 196 del 30 giugno 2003, da parte del Comune di Segrate.**

IL SINDACO

Premesso che l'art. 4, comma 1, del Dlgs 196/2003 definisce "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";

Considerato che il Dlgs 196/2003 impone una serie di adempimenti a carico del titolare, tra cui l'adozione del cosiddetto "Documento Programmatico sulla Sicurezza";

Richiamato l'art. 18 del Dlgs 196/2003 che limita il trattamento da parte di soggetti pubblici al solo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge e dai regolamenti;

Preso atto, inoltre, che ai sensi dell'art. 20, comma 1, del Dlgs 196/2003, il trattamento di dati sensibili è consentito solo se autorizzato da espressa disposizione di legge, nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite;

Ritenuto opportuno individuare con successivo atto, nell'ambito dell'Amministrazione Comunale, i responsabili del trattamento effettuato presso ciascuna Direzione;

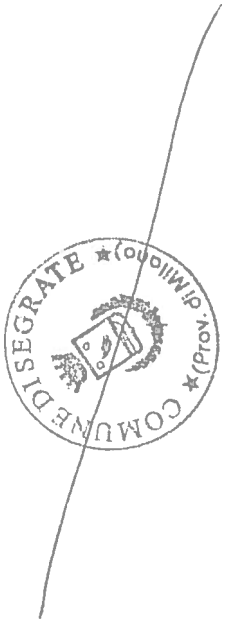
Tutto ciò premesso, in qualità di titolare, per il Comune di Segrate, del trattamento dei dati personali ai sensi del Dlgs 196/2003

ADOTTA

il "Documento Programmatico sulla Sicurezza dei dati personali", allegato al presente, quale parte integrante e sostanziale.

IL SINDACO
Adriano Alessandrini

Palazzo Comunale
via I Maggio 20090 - Segrate
Telefono 02/26.902.1 **Fax** 02/21.33.751
C.F. 83503670156 - **P.I.** 01703890150


COMUNE DI SEGRATE
(Prov. di Milano)

Città di Segrate

COMUNE DI SEGRATE (Prov. di Milano)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(DECRETO LEGISLATIVO 30 GIUGNO 2003, n. 196)

TITOLARE DEI DATI: COMUNE DI SEGRATE

Rif. int.	: DPS
File	: Documento programmatico sulla sicurezza dei dati personali.doc
Approvazione	: Alessandrini Alessandro – Sindaco pro-tempore
Data	: 5 agosto 2010

Palazzo Comunale
via I Maggio 20090 - Segrate
Telefono 02/26.902.1 **Fax** 02/21.33.751
C.F. 83503670156 - **P.I.** 01703890150

Indice

Premessa

Nel corso degli anni le attività istituzionali svolte dagli uffici del Comune di Segrate sono divenute sempre più dipendenti dall'infrastruttura tecnologica ICT (Information & Communication Technology). Per questo motivo è necessario un elevato grado di disponibilità, affidabilità e sicurezza informatica in relazione ai trattamenti di dati ed informazioni contenuti negli archivi informatizzati dell'Ente.

Considerate però le caratteristiche di apertura che i moderni sistemi informativi presentano nei confronti del mondo esterno all'Amministrazione - ad esempio l'utilizzo abituale della rete Internet come strumento di ausilio nella ricerca di informazioni e di facilitazione nell'interscambio informativo con altri soggetti – l'attuale stato dell'arte della tecnologia ICT considera i sistemi informativi come oggetti potenzialmente esposti a diversi rischi legati alle intrusioni informatiche, cioè alla possibilità che persone non autorizzate possano ottenere un qualche tipo di accesso agli archivi presenti sui sistemi gestiti dal Comune.

Inoltre un ulteriore rischio da non sottovalutare è quello che i sistemi informativi comunali, anche se posti in condizioni di sicurezza a livello minimale, possano fungere da rilancio per azioni lesive verso altri soggetti. Da questo punto di vista ad oggi, nonostante non sia prevedibile quale sarà l'orientamento della legislazione al riguardo, non è escluso che la negligenza nei confronti degli aspetti organizzativi e tecnologici riguardanti la sicurezza informatica sia vista come "colpa" a carico delle figure preposte al trattamento dei dati personali (Titolare, Responsabile, Incaricato).

Per questi motivi il Comune di Segrate ha deciso di implementare un Sistema di Gestione della Sicurezza delle Informazioni conforme alla norma ISO 27001, che consente di elevare il proprio livello di sicurezza nel trattamento delle informazioni rispetto a quanto previsto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

Il Comune di Segrate, quale Titolare del trattamento dei dati, ha redatto il presente regolamento in osservanza a quanto prescritto all'art. 34 del citato Decreto Legislativo 30 giugno 2003, n. 196 ed all'Allegato B) allo stesso, relativamente al Documento Programmatico sulla Sicurezza.

1 – Scopo del presente documento

Il presente documento disciplina le modalità di attuazione, nell'ambito del Comune di Segrate, delle disposizioni definite dall'art. 18 e dall'art. 20, commi 2 e 3, e dall'art. 181, comma 1, lett. a) del D.Lgs. del 30 Giugno 2003, n. 196.

Le disposizioni del presente documento garantiscono il trattamento di informazioni a carattere personale e sensibile, acquisite dall'Amministrazione o ad esso rese, riguardanti persone fisiche o giuridiche, secondo criteri coerenti con la normativa in materia di tutela dei dati personali.

2 – Campo di applicazione

Il presente documento si applica a tutti i soggetti che operano trattamenti di dati personali per conto del titolare, Comune di Segrate, ai sensi del D.Lgs. 30 giugno 2003, n. 196.

3 – Sintesi del contesto normativo

Il contesto normativo che regola gli aspetti relativi al trattamento ed alla sicurezza dei dati personali è rappresentato dal D.Lgs. del 30 Giugno 2003, n. 196, il quale, in particolare, riporta all'art. 4, comma 1, le seguenti definizioni:

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

b) "**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) "**dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;

d) "**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;

e) "**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. 213, 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 articoli60 e 61 del codice di procedura penale;

f) "**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;

g) "**responsabile**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) "**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) "**banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q)"**Garante**", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

Si riportano inoltre le ulteriori definizioni di cui all'art. 4, comma 2, del predetto Decreto Legislativo:

a) "**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) "**chiamata**", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) "**reti di comunicazione elettronica**", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) "**rete pubblica di comunicazioni**", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) "**servizio di comunicazione elettronica**", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

m) "**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.

Si riportano le ulteriori definizioni di cui all'art. 4, comma 3, del predetto Decreto Legislativo:

a) "**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 previsti nell'articolo 31;

b) "**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;

e) "**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g) "**sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Si riporta infine la definizione contenuta nel provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 pubblicata nella G.U. nr. 300 del 24 dicembre 2008:

Con la definizione di "**amministratore di sistema**" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento però

vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Per completezza di informazione, si citano i seguenti articoli tratti dal D.Lgs. 30 Giugno 2003, n. 196, in quanto rilevanti ai fini della lettura del presente regolamento:

Art. 31

"I dati personali oggetto di trattamento sono 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.".

Art. 33

"Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad 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.".

Art. 34

"Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari."

Si riportano infine i seguenti punti tratti dal Disciplinare Tecnico in Materia di Misure Minime di Sicurezza di cui all'Allegato B) del D.Lgs. 30 Giugno 2003, n. 196, in quanto descrittivi dei contenuti del Documento Programmatico sulla Sicurezza:

19. 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 contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di 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 ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

4 – Trattamento dei dati

I dati personali sono trattati secondo le modalità stabilite dall'art. 11, D.Lgs. 30 giugno 2003, n. 196.

I dati in possesso del Comune di Segrate sono di norma trattati in forma elettronica o mediante l'ausilio di sistemi automatizzati.

Le disposizioni del presente documento si applicano, in quanto compatibili, al trattamento dei dati in forma non automatizzata.

Ad eccezione delle ipotesi di trasferimento di dati per il puro adempimento di obblighi di legge, è esclusa la messa a disposizione o la consultazione di dati in blocco o la ricerca per nominativo di tutte le informazioni contenute nella banca dati, senza limiti di procedimento o di settore.

L'elenco dei trattamenti sia interni che esterni è contenuto nell'Allegato D al presente documento.

5 – Informazione

A cura del titolare o degli incaricati al trattamento, viene data ampia diffusione degli obblighi informativi di cui all'art. 13 del D.Lgs. 30 giugno 2003, n. 196.

6 – Diritti dell'interessato

Le richieste per l'esercizio dei diritti di cui all'art. 7 del D.Lgs. 30 giugno 2003, n. 196 sono presentate all'Ufficio Relazioni con il Pubblico del Comune di Segrate, secondo le modalità stabilite all'art. 9 dello stesso Decreto Legislativo.

Nelle ipotesi in cui, per il trattamento dei dati, sia necessario il consenso dell'interessato, il medesimo consenso è prestato in forma scritta, anche mediante l'utilizzo di strumenti informatici e telematici.

7 – Attività che preseguono rilevanti finalità di interesse pubblico

Ai fini del presente documento si intendono per attività che perseguono rilevanti finalità di interesse pubblico tutte quelle svolte dal Comune di Segrate in relazione a funzioni e compiti a esso attribuiti, delegati o conferiti dalla normativa statale e regionale vigente, nonché quelle inerenti all'organizzazione dell'Amministrazione e allo sviluppo dell'attività amministrativa, nei suoi vari profili.

Le attività che perseguono rilevanti finalità di interesse pubblico sono individuate, per il trattamento dei dati sensibili, dal D.Lgs. 30 Giugno 2003, n. 196, da altre leggi e dal Garante, in base a quanto previsto al Capo IV, Titolo IV dello stesso Decreto Legislativo.

8 – Trattamento di dati sensibili che non perseguono finalità di interesse pubblico

Per favorire l'individuazione delle attività istituzionali non correlabili a rilevanti finalità di interesse pubblico date nel D.Lgs 30 giugno 2003, n. 196, e per consentire al Garante per la protezione dei dati personali di adottare specifici provvedimenti ai sensi dell'art. 20 dello stesso Decreto Legislativo, l'Amministrazione:

1. *verifica la rilevanza delle attività istituzionali comportanti il trattamento di dati sensibili in relazione al buon andamento dell'attività amministrativa;*
2. *verifica quali di queste attività non possono essere ricondotte al quadro di riferimento dettato dal suindicato decreto legislativo;*
3. *individua e configura la rilevanza dell'interesse pubblico perseguito con la particolare attività istituzionale.*

L'Amministrazione comunica al Garante per la protezione dei dati personali i trattamenti di dati sensibili individuati per i quali non è determinata dalla legge una corrispondente rilevante finalità di interesse pubblico.

Le modalità di comunicazione al Garante sono definite dal Sindaco pro-tempore nelle disposizioni organizzative di cui al successivo punto 9 del presente documento.

9 – Individuazione delle tipologie e delle caratteristiche dei trattamenti dati

A fronte delle rilevanti finalità di interesse pubblico individuate dalla legge o dal Garante, in assenza della definizione delle tipologie di dati e delle operazioni eseguibili, per poter eseguire il corretto svolgimento delle attività istituzionali il Comune provvede a determinare quali tipi di dati sono trattabili e quali forme di gestione su di essi possano essere realizzate.

Il Titolare dei dati attraverso il presente documento e i relativi allegati, individua i tipi di dati personali comuni e sensibili correlabili alle rilevanti finalità di interesse pubblico date dalla legge o dal Garante. Al contenuto del presente documento è data massima diffusione presso le direzioni dell'Amministrazione e nelle relazioni della stessa con la comunità locale, con soluzioni differenziate, ivi comprese quelle comportanti l'utilizzo delle reti telematiche e dei mezzi di comunicazione di massa.

L'aggiornamento del quadro di riferimento per le tipologie di dati personali normali e sensibili assoggettabili a trattamento secondo le garanzie del D.lgs. 30 giugno 2003, n. 196 e per le operazioni su di essi eseguibili, viene effettuato almeno annualmente entro il 31 marzo dal Titolare con proprio provvedimento. Ogni trattamento verrà riepilogato nelle schede denominate ELTRDP allegate al presente Documento Programmatico per la Sicurezza.

L'aggiornamento dovrà essere fatto qualora innovazioni normative, tecnologiche o rilevanti trasformazioni di carattere gestionale rendano necessaria l'individuazione di nuove tipologie di dati o di operazioni eseguibili.

Nell'informativa resa ai sensi dell'art. 7 del D.lgs 30 giugno 2003 n. 196, ai soggetti che conferiscono dati all'Amministrazione per lo svolgimento di un'attività istituzionale, sono fornite tutte le indicazioni inerenti alla corrispondente rilevante finalità di interesse pubblico perseguita, i tipi di dati personali normali e sensibili per i quali risulta necessario attivare un trattamento e le operazioni eseguibili sui medesimi dati.

10 – Distribuzione compiti e responsabilità

Il Titolare dei trattamenti è il Comune di Segrate, rappresentata legalmente dal Sindaco pro-tempore.

Il D.Lgs. 30 giugno 2003, n. 196 (art. 4, comma 1, lettera f) definisce "titolare" la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro Istituto, 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.

Poiché il Dlgs 196/2003 da facoltà al titolare dei dati di nominare i responsabili dei trattamenti (art. 29), tenendo conto della realtà delComune di Segrate, questi vengono individuati e nominati con provvedimento allegato al presente (Allegato B).

Il Responsabile dei dati:

1. *cura il coordinamento di tutte le operazioni di trattamento di dati affidate agli Incaricati del trattamento appartenenti alla struttura organizzativa che sovrintende;*
2. *provvede a dare istruzioni agli Incaricati al fine della corretta elaborazione dei dati personali normali e sensibili;*
3. *procede alle verifiche sulla metodologia di introduzione e di gestione dei dati, anche attraverso controlli a campione da eseguirsi periodicamente;*
4. *è responsabile dei procedimenti di rettifica dei dati;*
5. *applica tutte le disposizioni operative per la sicurezza della banca dati e l'adozione delle misure di sicurezza contenute nelle singole procedure allegate del presente documento;*
6. *cura la realizzazione delle singole banche dati cui sovraintende con la funzione organizzativa del Comune che gestisce il sistema informativo comunale;*
7. *cura la comunicazione agli interessati del trattamento dei dati e la loro diffusione;*
8. *dà ampia diffusione degli obblighi informativi di cui all'art. 13 del D.Lgs. 30 Giugno 2003, n. 196;*
9. *individua in un apposito elenco, allegato al presente, i soggetti incaricati del trattamento, da svolgersi secondo le modalità di cui agli art. 11 e 13 del D.Lgs. 30 Giugno 2003, n. 196;*
10. *dispone il blocco dei dati, qualora sia necessaria una sospensione temporanea delle operazioni di trattamento.*

Nella ipotesi di blocco dei dati o dell'accesso ai medesimi attraverso reti di trasmissione ad alta velocità o terminali accessibili al pubblico, il Responsabile ne dà tempestiva comunicazione al Titolare.

Sono stati individuati e sono elencati nell'Allegato "A" gli incaricati al trattamento dei dati.

Gli incaricati al trattamento dei dati:

1. trattano tutti i dati personali di cui vengono a conoscenza nell'ambito delle proprie funzioni, in modo lecito e secondo correttezza;
2. effettuano la raccolta, l'elaborazione, la registrazione ecc. di dati personali esclusivamente per lo svolgimento delle proprie mansioni;
3. accedono unicamente alle banche dati per le quali sono stati espressamente incaricati con lettera di incarico;
4. evitano di creare banche dati nuove senza espressa autorizzazione del titolare;
5. mantengono assoluto riserbo sui dati personali di cui vengono a conoscenza nell'esercizio delle proprie funzioni;

6. evitano di asportare supporti informatici o cartacei contenenti dati personali di terzi senza la previa autorizzazione del titolare.

11 – Analisi dei rischi

Per quanto riguarda l'analisi dei rischi che incombono sui dati si fa riferimento all'analisi annuale che viene effettuata nell'ambito delle attività del Sistema di Gestione per la Sicurezza delle Informazioni, a cui si rimanda.

12 – Misure di sicurezza

Le misure adottate per il trattamento in sicurezza dei dati dal Comune di Segrate, previste dal Disciplinare Tecnico contenuto nell'Allegato B del D.Lgs. 30 Giugno 2003, n. 196, richiamato dall'articolo 34 dello stesso, sono descritte di seguito:

Autenticazione informatica

Procedura PRO002 - Gestione password di qualità
Procedura PRO003 - Gestione degli accessi alla rete

Credenziali di autenticazione

Procedura PRO002 - Gestione password di qualità
Procedura PRO003 - Gestione degli accessi alla rete

Sistema di autorizzazione

Procedura PRO003 - Gestione degli accessi alla rete
Procedura PRO004 - Gestione degli accessi ad Internet
Procedura PRO005 - Gestione degli accessi alla posta elettronica
Procedura PRO011 - Gestione degli accessi agli applicativi

Sistema di accesso

Procedura PRO009 - Gestione del posto di lavoro e dell'accesso alle strutture
Procedura PRO012 - Sicurezza nell'accesso di terze parti

Copie di sicurezza e ripristino della disponibilità dei dati e dei sistemi

Procedura PRO007 - Classificazione delle informazioni
Manuale IT – Scheda 001 Backup delle informazioni

Supporti di memorizzazione

Procedura PRO007 - Classificazione delle informazioni

Piano di continuità

Procedura PRO019 - Business continuity

Antivirus

Il software antivirus installato sulle postazioni, viene gestito centralmente utilizzando un modulo specifico della suite Landesk ver.9.00. L'aggiornamento delle firme avviene in modo automatico e in maniera totalmente trasparente per l'utente finale. Una volta la settimana viene avviata la scansione dei dati contenuti sulle postazioni al fine di rimuovere eventuali file infetti.
Esiste inoltre un sistema antivirus dedicato sul server di posta elettronica e un altrettanto Sistema antivirus sulle porte del firewall. Tali sistemi vengono aggiornati automaticamente ogni giorno.

13 – Formazione e addestramento

La previsione degli 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 ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal Comune di Segrate è specificata nella procedura "SGQ P04 Formazione del personale".

14 – Trattamenti affidati a terzi esterni alla struttura

La descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del Titolare, è contenuta nella procedura "PRO012 - Sicurezza nell'accesso di terze parti".

15 – Amministratori di sistema

Il provvedimento del Garante per il trattamento dei dati personali del 27 novembre 2008 pubblicato nella Gazzetta Ufficiale nr. 300 del 24 dicembre 2008, modificato e integrato dal provvedimento del 25 giugno 2009, ha rammentato ai titolari di trattamento di dati personali la particolare criticità del ruolo di amministratore di sistema. Nel provvedimento vengono anche indicati i requisiti professionali e di sicurezza che un amministratore di sistema deve soddisfare.
Tenendo conto di quanto indicato, è stata effettuata una valutazione dei requisiti di tutti gli amministratori di sistema presenti in nel Comune di Segrate ed è stata riformulata la lettera di incarico.
Per quanto riguarda il punto 2 C secondo comma, ove viene stabilito che, qualora l'attività degli amministratori di sistema riguardi servizi o sistemi che trattano informazioni di carattere personale dei lavoratori, i titolari sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema.
La direzione Centrale e Controllo di gestione comunicherà formalmente i nominativi degli amministratori di sistema a qualsiasi dipendente ne faccia esplicita richiesta.

Per quanto attiene alla registrazione degli accessi (punto 2 f del provvedimento citato), si procede nel seguente modo:

- *client – viene attivata la registrazione dei log di accesso degli amministratori di sistema localmente. Si ritiene infatti che, dato il livello medio di conoscenze informatiche dei dipendenti e dato che il profilo di autorizzazione non consente loro di accedere a determinate funzionalità del sistema operativo, questa metodologia goda di sufficienti garanzie di integrità;*
- *server – viene adottato un sistema di centralizzazione dei log che prevede la conservazione degli stessi in modo che non siano modificabili.*

16 – Documenti di riferimento

- *Organigramma vigente – Allegato A o vedere ultima delibera di giunta di approvazione organigramma*
- *Nomina responsabili del trattamento –*
- *Elenco degli incaricati al trattamento dati –dotazione organica alla data*
- *Elenco dei trattamenti –*
- *Elenco dei terzi incaricati –*
- *Elenco degli amministratori di sistema –*
- *Analisi del rischio – Analisi allegata alla documentazione del SGSI*
- *Misure di sicurezza – Procedure indicate al punto 12*
- *Elenco dei sistemi – Allegato 2 alla Dichiarazione di ambito del SGSI*
- *DPS Video Sorveglianza Polizia Locale*
- *Elenco incaricati (DPS Video Sorveglianza Polizia Locale)*

COPIA CONFORME
ALL'ORIGINALE
COMPOSTA DA N. 15
FACCIATE.
Segrate li 5.8.2010
L'ISTRUTTORE DIRETTIVO AMMINISTRATIVO
D.ssa Emanuela Zanini