COMUNE di MALETTO
(Prov. Catania)

DECRETO LEGISLATIVO
30 giugno 2003 n. 196
Codice in materia di protezione dei dati personali

REGOLAMENTO SULLA TUTELA DELLA RISERVATEZZA DEI DATI PERSONALI

APPROVATO CON DELIBERAZIONE DEL CONSIGLIO COMUNALE N. 13 DEL 26/04/2005

Sommario

Articolo 1 – Oggetto e finalità

Il presente Regolamento per il trattamento dei dati personali, in attuazione al Decreto Legislativo n. 196 del 30 giugno 2003, disciplina il trattamento, la comunicazione e la diffusione, da parte del Comune di Maletto con sede in Maletto (CT) via Umberto n. 1/A, dei dati personali contenute nelle banche dati di cui l'amministrazione comunale è Titolare.
Il Comune gestisce le banche dati di cui è titolare, trattati sia con sistemi automatizzati che non automatizzati, esclusivamente per l'esercizio delle funzioni

previste dalla legge, dai regolamenti e dal proprio Statuto o nell'ambito di eventuali accordi tra enti pubblici intesi a favorire la trasmissione dei dati nei limiti degli art. 18, 19, 20, 21 e 22 del Decreto Legislativo 30 giugno 2003, n. 196.

Articolo 2 – Definizioni di riferimento

Ai fini del presente Regolamento, si applicano le seguenti definizioni elencate nel Decreto Legislativo 196/2003:
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;
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;
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;
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;
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;
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;
incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

informativa: dichiarazione scritta che deve essere resa all'interessato prima di iniziare un'operazione di trattamento di dati che lo riguardano. Contiene, tra le altre cose, l'indicazione delle finalità e delle modalità del trattamento e il riferimento ai soggetti ai quali i dati possono essere comunicati e all'ambito della loro diffusione.
consenso: dichiarazione di volontà con la quale l'interessato autorizza il titolare ad effettuare una o più operazioni di trattamento secondo le indicazioni fornite con l'informativa.
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;
diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
Garante: l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
Ai fini del presente Regolamento si intende, inoltre, per:
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;
chiamata: la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
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;
rete pubblica di comunicazioni: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

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;
abbonato: qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
dati relativi al traffico: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
dati relativi all'ubicazione: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
servizio a valore aggiunto: il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
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.
Ai fini del presente Regolamento si intende, altresì, per:
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;
strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
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;
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;

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;
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.

Articolo 3 – Titolare, Responsabili, Incaricati

Il Comune di Maletto è il titolare dei trattamenti dei dati personali gestiti dalle proprie articolazioni organizzative e delle banche-dati ad esse afferenti. Al Sindaco, legale rappresentante dell'ente spettano gli adempimenti che la legge affida al "Titolare".
I Responsabili degli uffici e dei servizi individuati dal Sindaco sono responsabili dei trattamenti nell'ambito dei rispettivi settori. Il Titolare può comunque designare con apposito provvedimento uno o più "responsabili" diversi dai predetti soggetti, ai sensi dell'art. 29 del Decreto Legislativo 30 giugno 2003, n. 196.
Il Titolare oppure il responsabile provvede, all'individuazione degli "incaricati del trattamento".

Articolo 4 – Individuazione delle banche dati

Le banche dati di cui all'art. 4 della del Decreto Legislativo 30 giugno 2003, n. 196, gestite dall'Amministrazione Comunale, sono individuate su indicazione dei Responsabili del trattamento.
Le banche dati di cui al presente regolamento sono gestite in forma elettronica e cartacea.
L'Amministrazione Comunale, di regola, provvede annualmente, alla verifica ed all'aggiornamento dell'elenco delle banche dati dei trattamenti sulla base delle relative comunicazioni inoltrate dai responsabili del trattamento.

Articolo 5 – Modalità di raccolta e requisiti dei dati personali

Il trattamento dei dati deve avvenire in modo lecito e secondo correttezza. I dati devono possedere i requisiti dell'esattezza, della pertinenza, della completezza, dell'aggiornamento rispetto alle finalità della raccolta e del successivo trattamento, della non eccedenza rispetto alle finalità per cui sono trattati e della conservazione limitatamente agli scopi del trattamento.
Con riferimento alle modalità di raccolta i dati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi.

Le disposizioni del presente regolamento si applicano al trattamento dei dati automatizzato e, in quanto compatibili, al trattamento dei dati non automatizzato.

Articolo 6 – Trattamento dei dati personali

Il trattamento dei dati personali da parte del Comune di Maletto, svolto sia mediante l'ausilio di mezzi elettronici e comunque informatizzati, sia cartacei, è consentito esclusivamente per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla normativa vigente in materia di trattamento dei dati personali, dal presente Regolamento e dalle direttive del Garante.
Nell'ambito del trattamento dei dati sensibili e giudiziari, di cui agli artt. 20, 21 e 22 del Decreto Legislativo 30 giugno 2003, n. 196, l'Ente si attiene ai seguenti principi:
- il massimo rispetto della dignità dell'interessato, agevolando l'esercizio dei diritti di cui all'art. 7 del Decreto Legislativo 30 giugno 2003, n. 196 (accesso, correzione dati, opposizione al trattamento, ecc.);
- si possono svolgere soltanto le operazioni strettamente necessarie al perseguimento della finalità sottesa al trattamento (principio di necessità del trattamento dei dati art. 3 del Decreto Legislativo 30 giugno 2003, n. 196).
Il trattamento dei dati sensibili è consentito ai soggetti pubblici nei seguenti casi:
a) se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi dì dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite;
b) nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo;
c) Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2;
La comunicazione/diffusione dei dati deve avvenire nel rispetto delle disposizioni legislative e regolamentari sulla riservatezza, da combinarsi con le norme di diritto positivo in materia di accesso ai documenti amministrativi.
Nelle ipotesi in cui la legge, lo statuto o il regolamento prevedano pubblicazioni obbligatorie, il responsabile del procedimento adotta le misure eventualmente

necessarie per garantire la riservatezza dei dati sensibili, di cui all'art. 20 del Decreto Legislativo 30 giugno 2003, n. 196.

I trattamenti senza l'ausilio di strumenti elettronici

Il Decreto Legislativo 196/2003 disciplina gli aspetti riguardanti:

l'affidamento di atti o documenti contenenti dati personali agli incaricati, e la custodia da parte di questi (lettera b) del comma 1 dell'art. 35 del Codice, cui danno concreta attuazione i punti 27 e 28 del disciplinare tecnico);

le creazione e gestione degli archivi, nei quali riporre e custodire atti e documenti contenenti dati personali quando gli stessi non sono utilizzati per lo svolgimento delle operazioni affidati agli incaricati (lettera c) del comma 1 dell'art. 35 del Codice, cui da attuazione il punto 29 del disciplinare tecnico).

Nel rispetto di quanto prescritto dal punto 27 del disciplinare tecnico agli incaricati vengono impartite istruzioni scritte su come deve avvenire il controllo e la custodia di atti e documenti contenenti dati personali di qualsiasi natura.

Gli incaricati del trattamento prelevati dagli archivi i soli atti e documenti loro affidati, li devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine delle operazioni loro affidate.

Il controllo e la custodia devono avvenire in modo tale, come prescrive il punto 28 del disciplinare, in presenza di atti e documenti contenenti dati sensibili o giudiziari, che ai dati non accedano persone prive di autorizzazione. A tale fine sarà cura di ogni incaricato riporre nel cassetto della propria scrivania, che verrà chiuso a chiave, i documenti in suo possesso, prima di assentarsi, anche temporaneamente, dal posto di lavoro.

Seguendo i dettami del punto 29 del disciplinare tecnico gli atti e documenti contenenti dati sensibili e giudiziari sono conservati in archivi ad accesso controllato secondo i seguenti accorgimenti:

gli incaricati preventivamente autorizzati ad accedere agli archivi richiedono la chiave degli stessi al custode e la restituiscono al termine dell'accesso;

al termine dell'orario lavorativo, i nominativi di chi accede all'archivio verranno annotati in un apposito registro.

I trattamenti con strumenti elettronici

L'articolo 34 del codice e i punti da 1 a 26 del disciplinare tecnico prescrivono le misure minime di sicurezza da applicare per i trattamenti effettuati con strumenti elettronici.

Il primo ordine di prescrizioni, dettate dal primo comma dell'art. 34 del codice, impone che vengano adottati gli opportuni sistemi, al fine di consentire l'accesso agli strumenti elettronici solo a chi è autorizzato, tramite:

lettera a) l'impostazione di un sistema di autenticazione informatica, che l'articolo 4, comma 3, lettera c) del codice definisce come l'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità.

lettera b) l'adozione di procedure di gestione delle credenziali di autenticazione, che l'articolo 4, comma 3, lettera d) definisce come i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

Per realizzare la credenziale di autenticazione (cioè la chiave per accedere allo strumento elettronico), l'istituto ha associato un codice per l'identificazione dell'incaricato (username), attribuito dal responsabile del sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che egli stesso provvede ad elaborare, mantenere riservata e modificare periodicamente.

Il secondo ordine di prescrizioni, previste dal comma 34, disciplina l'impostazione del sistema di autorizzazione, che la lettera g) del comma 3 dell'articolo 4 definisce come 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. A tale fine, è previsto l'obbligo di:

lettera c) utilizzare un sistema di autorizzazione.

lettera d) aggiornare periodicamente l'individuazione dell'ambito del trattamento consentito ai singoli incaricati, e agli addetti alla gestione o alla manutenzione degli strumenti elettronici.

Rispettando i dettami del punto 13 e 14 del disciplinare tecnico viene limitato preventivamente l'accesso di ciascun incaricato ai soli dati necessari per effettuare le operazioni di trattamento, che si rendono indispensabili per svolgere le mansioni lavorative. Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

L'articolo 34 del codice privacy impone di:

lettera e) proteggere gli strumenti elettronici ed i dati, rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici.

lettera f) adottare procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Il punto 16 del disciplinare prevede l'obbligo di proteggere i dati personali *contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615- quinquies del codice penale,* aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Si tratta dei *virus*, dai quali la norma impone di difendersi, attivando idonei strumenti elettronici, da aggiornare con cadenza almeno semestrale.

Il punto 20 aggiunge l'obbligo di adottare una ulteriore misura, in caso di trattamento di *dati sensibili o giudiziari*, imponendo di proteggerli *dall'accesso abusivo*, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici. Ai sensi dell'articolo 615-ter del codice penale, pone in essere un accesso abusivo chi *si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*.

La norma prevede che, nel caso in cui si trattino dati sensibili o giudiziari, non ci si possa limitare a difendersi dai programmi, ma si debbano utilizzare idonei strumenti elettronici di protezione perimetrale (ad esempio, *firewall*), per proteggersi contro l'ipotesi, ancora più pericolosa, in cui la *mente criminale* stessa tenti di accedere direttamente.

I Firewall sono dei sistemi hardware e software, dislocati nei punti di interconnessione tra reti TCP/IP distinte, che hanno il compito di controllare gli accessi alle risorse di rete interconnesse: tale controllo è effettuato filtrando i messaggi in transito e facendo passare solo quelli che rispondono ai requisiti definiti dalle politiche di sicurezza.

Il punto 17 prevede che, *in tutti i casi*, ci si debba dotare anche di programmi, la cui funzione è di:

• prevenire la vulnerabilità degli strumenti elettronici, non solo e non necessariamente per effetto di attacchi esterni;

• correggere i difetti insiti negli strumenti stessi.

Tra i principali punti di debolezza di un sistema informatico vanno sicuramente annoverati il sistema operativo e le applicazioni, sfruttando gli eventuali errori *(bug*) presenti nei quali degli estranei potrebbero, tra l'altro, riuscire a guadagnare l'accesso al sistema. Le contromisure da adottare sono essenzialmente di due tipi:

l'aggiornamento costante dei prodotti, non appena viene scoperto un *bug*, tale procedura è nota come installazione di *patch* la verifica periodica dell'installazione e della configurazione dei prodotti software.

Sono disponibili dei programmi in grado di verificare automaticamente eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete: la norma prevede che gli ***aggiornamenti di tali programmi*** debbano essere effettuati con cadenza almeno annuale (che diviene semestrale, in caso di trattamento di dati sensibili o giudiziari), nell'ambito di un *test generale* per verificare il corretto funzionamento dell'intero sistema.

Per quanto concerne il salvataggio dei dati, al fine di consentirne il *recupero*, al verificarsi di eventi atti a distruggerli, il punto 18. prescrive che, in tutti i casi, debbano essere impartite istruzioni organizzative e tecniche, che prevedono il salvataggio dei dati *con frequenza almeno settimanale.* Per i dati *sensibili e giudiziari* il punto 23 aggiunge la prescrizione, per cui l'organizzazione deve essere in grado di provvedere, in ogni caso, al ripristino dei dati *entro sette giorni*. L'istituto ha nominato

degli incaricati del backup che effettuano, periodicamente (settimanalmente), un copia di tutti i dati presenti nel sistema su dispositivi opportuni. In caso di guasto hardware dei dischi è quindi possibile ripristinare il sistema nello stesso stato in cui si trovava nel momento dell'ultimo backup.
In ottemperanza dei punti 21 e 22 del disciplinare, una particolare attenzione è stata dedicata ai supporti rimovibili contenenti dati sensibili o giudiziari, applicando le seguenti misure:
• sono custoditi ed utilizzati in modo tale da impedire accessi non autorizzati e trattamenti non consentiti: sono impartite istruzioni affinché essi vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente *formattati* quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
• una volta cessate le ragioni per la conservazione dei dati i supporti non vengono *abbandonati* ma vengono posti in essere gli opportuni accorgimenti, anche con la distruzione del supporto, finalizzati a rendere ***inintelligibili e non ricostruibili tecnicamente i dati*** in essi contenuti, al fine di impedire che essi vengano *carpiti* da persone non autorizzate al trattamento.

Articolo 7 – *Scambio di dati con altri soggetti pubblici*

Il Comune favorisce la trasmissione di dati o documenti tra le banche dati e gli archivi degli enti territoriali, degli enti pubblici, dei gestori e degli incaricati di pubblico servizio operanti nell'ambito dell'Unione Europea, nel rispetto del diritto alla riservatezza con particolare riferimento alla tutela dei dati sensibili.
La trasmissione dei dati può avvenire anche attraverso sistemi informatici e telematici, reti civiche, nonché mediante l'utilizzo di reti di trasmissione dati ad alta velocità.
La trasmissione di dati o documenti dovrà essere, di norma, preceduta da uno specifico protocollo d'intesa che contenga, di norma, l'indicazione del titolare e del responsabile della banca dati e delle operazioni di trattamento, nonché le modalità di connessione, di trasferimento e di comunicazione dei dati e le misure di sicurezza adottate.

Articolo 8 – Informativa

L'informativa agli interessati è un atto con cui chi tratta i dati altrui, innanzitutto, si identifica; inoltre, rende noto agli interessati le caratteristiche del trattamento e illustra i diritti riconosciuti dalla legge. E' un atto, orale o scritto, che deve precedere il trattamento, privo di particolari formalità, ma deve essere idoneo allo scopo perseguito.
É possibile utilizzare formule colloquiali per evidenziare, anche in modo sintetico ma senza lacune o ambiguità, alcune circostanze che riguardano le finalità e le modalità

del trattamento cui sono destinati i dati, la natura obbligatoria o facoltativa del loro conferimento, le conseguenze dell'eventuale rifiuto di rispondere, i soggetti e le categorie di soggetti ai quali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, l'ambito di diffusione dei dati medesimi, i diritti dell'interessato (art. 7 del Codice) e gli estremi identificativi del titolare e degli eventuali responsabili del trattamento, se designati.
Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato, in caso di esercizio dei diritti, è indicato tale responsabile.
Al fine di dare ampia diffusione alle informazioni di cui all'art. 13 del D. Lgs. 196/2003 il titolare ed il responsabile del trattamento favoriscono tale informativa attraverso l'adozione di uno o più strumenti quali:
- messa a disposizione presso gli uffici di fogli recanti le informazioni di cui all'art. 13 del D. Lgs. 196/2003;
- cartelli affissi nei locali dove gli interessati si recano;
- inserimento delle informazioni nei moduli già predisposti dall'ente;
- messaggi sul sito Internet dell'ente.

Articolo 9 – Diritti dell'interessato

All'interessato, i cui dati sono contenuti in una banca di dati del Comune di Maletto, spettano i diritti di cui all'art. 7 del Decreto Legislativo 196/2003 e cioè:

di essere informato su quanto indicato in merito ai dati previsti per la notificazione;

di ottenere, a cura del titolare o del responsabile, senza ritardo;

la conferma dell'esistenza o meno di trattamenti di dati personali che lo riguardano, anche se non ancora registrati, e la comunicazione in forma intelligibile dei medesimi dati e della loro origine, nonché della logica e delle finalità del trattamento; la richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni;

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;

l'aggiornamento, la rettificazione, ovvero, qualora vi abbia interesse, l'integrazione dei dati;

l'attestazione che le operazioni di cui ai numeri 2. e 3. 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 riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

di opporsi, in tutto o in parte, al trattamento di dati personali che lo riguardano, previsto a fini di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva e di essere informato dal titolare, non oltre il momento in cui i dati sono comunicati o diffusi, della possibilità di esercitare gratuitamente tale diritto.

L'interessato può esercitare tali diritti con una richiesta scritta al Titolare della banca di dati. La richiesta sarà ritenuta valida anche se effettuata da persone terze o associazioni munite di delega o procura scritta dell'interessato.

L'esame delle istanze per l'esercizio dei diritti compete al Responsabile del trattamento dati.

In caso di inerzia o contro il provvedimento del Responsabile del trattamento, l'interessato può proporre ricorso al Garante o all'Autorità Giudiziaria ai sensi dell'art. 56 del Decreto Legislativo 30 giugno 2003, n. 196.

Qualora, in seguito alla richiesta dell'interessato di conoscere l'esistenza di trattamenti di dati che lo riguardano, risulti l'inesistenza degli stessi, l'interessato sarà tenuto al pagamento di un contributo spese non superiore ai costi effettivamente sostenuti dall'ente.

Articolo 10 – Misure di sicurezza

I Responsabili ed il Titolare del trattamento dei dati provvedono, in relazione alla disciplina disposta del Decreto Legislativo 30 giugno 2003, n. 196, all'adozione di misure di sicurezza al fine di prevenire:

- i rischi di distruzione, perdita di dati o danneggiamento delle banche dati o dei locali ove esse sono collocate;
- l'accesso non autorizzato ai dati stessi;
- modalità di trattamento dei dati non conformi alla legge o al regolamento;
- la cessione o la distruzione dei dati in caso di cessazione di un trattamento.

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze rese disponibili dal 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.

Articolo 11 – Il Documento Programmatico sulla Sicurezza

Il Comune di Maletto ha predisposto, trattando dati sensibili e/o giudiziari con l'utilizzo di strumenti elettronici, ai sensi dell'art. 34 lettera g) e come prescritto dal punto 19 del disciplinare tecnico, apposito documento programmatico sulla sicurezza dei dati.
Tale documento deve essere aggiornato annualmente entro il 31 marzo. In esso vengono definiti:
-l'elenco dei trattamenti di dati personali;
-la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
-l'analisi dei rischi che incombono sui dati;
-le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
-la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
-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;
-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;
-per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Articolo 12 – Verifiche e controlli

I responsabili del trattamento provvedono, con propri atti, a dar corso alle disposizioni organizzative in materia di dati personali e sensibili, nelle articolazioni cui sono preposti.
A cura del responsabile del trattamento dei dati sono attivati periodicamente controlli, anche a campione, al fine di garantire il rispetto delle misure di sicurezza relative ai vari trattamenti e l'attendibilità dei dati trattati.

Articolo 13 – Utilizzo dei dati all'interno degli uffici comunali

La comunicazione dei dati all'interno della struttura organizzativa del Comune, per ragioni d'ufficio e nell'ambito delle specifiche competenze, non è soggetta a limitazioni

particolari, salvo quelle espressamente previste da leggi e regolamenti. Non si considera comunicazione di dati a terzi la trasmissione e l'accesso di dati da parte del personale dipendente del Comune, qualora il trasferimento e l'accesso avvenga per ragioni di ufficio, nell'esercizio delle mansioni proprie di ciascun dipendente.
Il responsabile del trattamento dei dati, specie se la comunicazione concerne dati sensibili, può tuttavia disporre, con adeguata motivazione, le misure ritenute necessarie alla tutela della riservatezza delle persone, limitando l'accesso o la trasmissione dei dati sensibili ai soli casi di effettiva necessità per lo svolgimento delle funzioni ed attività comunali.

Articolo 14 – Comunicazione o diffusione dei dati

Una specifica attenzione va dedicata alle ipotesi di comunicazione o diffusione dei dati.
La comunicazione/diffusione dei dati è ammessa:
a) nei casi previsti dalla legge;
b) nei casi previsti dai regolamenti statali e comunali;
c) in altri casi in cui la comunicazione di dati a soggetti pubblici sia necessaria per lo svolgimento delle loro funzioni istituzionali, previa autorizzazione del Garante. Non è mai possibile comunicare dati ai privati fuori dai casi previsti sub "a" e "b".
Ogni richiesta di comunicazione di dati personali rivolta da privati deve essere scritta e motivata e deve indicare le norme di legge o di regolamento su cui si basa.
E' esclusa la messa a disposizione o la consultazione di dati in blocco e la ricerca per nominativo di tutte le informazioni contenute nella banca dati, senza limiti di procedimento o settore, ad eccezione delle ipotesi di trasferimento di dati tra enti pubblici o associazioni di categoria e di indagini di pubblica sicurezza.
In altri termini, ogni qual volta si prospetti l'eventualità di divulgare (in qualsiasi forma o modo) dati personali, è necessario procedere alle seguenti verifiche, specie se a riguardo di dati sensibili:
- verifica della legittimità della divulgazione alla luce della informativa fornita all'interessato;
- verifica di eventuali normative che consentano/rendano obbligatoria la divulgazione.

Una delle principali innovazioni della legge cd. "*sulla privacy*" è quella che prevede che il trattamento dei dati personali sia reso noto all'interessato nei suoi elementi essenziali, e si svolga entro gli stessi limiti. In altri termini, una volta che l'interessato viene informato delle modalità del trattamento dei suoi dati personali, detta informativa costituisce uno dei limiti del trattamento stesso.
Ciascun incaricato deve, pertanto, conoscere le informative che il Comune di Maletto fornisce in relazione ai trattamenti che effettua. E' chiaro che ogni incaricato avrà cura di valutare con maggiore attenzione le informative che più direttamente riguardano la sua attività.

Articolo 15 – Privacy e disposizioni sul diritto di accesso

Ai sensi dell'art. 59 del D.Lgs. 196/2003, le vigenti norme in materia di accesso ai documenti amministrativi sono fatte salve soltanto in quanto compatibili con la legge stessa.
Il responsabile del trattamento deve garantire il rispetto della riservatezza nell'ambito dei procedimenti di accesso ai documenti di pertinenza dei propri uffici ed è competente a valutare le richieste di accesso, sotto il profilo della ricevibilità e della ammissibilità delle stesse, a richiedere tempestivamente le integrazioni, a formulare e comunicare il diniego di accesso.
In particolare non saranno comunicati quei dati personali di soggetti terzi che non siano indispensabili per soddisfare la richiesta di accesso.
Riguardo alle richieste di accesso presentate dai consiglieri comunali e circoscrizionali la normativa vigente prevede che gli stessi hanno diritto di ottenere dagli uffici del Comune, nonché dalle aziende ed enti dipendenti tutte le notizie ed informazioni in loro possesso, utili all'espletamento del loro mandato. L'istanza di accesso dovrà contenere la precisazione dell'atto richiesto e delle informazioni in possesso dell'ente (indicazione degli estremi del documento oggetto della richiesta ovvero degli elementi che ne consentono l'individuazione).
I presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.
Nel caso in cui le richieste siano presentate per ragioni diverse si applicherà la normativa prevista dalla L. 241/90.
Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, ai sensi dell'art. 60 del D.Lgs. 196/2003, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Articolo 16 – Pubblicità degli atti amministrativi comunali

Al fine di tutelare la riservatezza delle persone nelle ipotesi in cui la legge, lo Statuto o i regolamenti prevedano la pubblicazione di atti e provvedimenti, il responsabile del trattamento deve adottare opportune misure per garantire la riservatezza dei dati (ad

es. omissis, rinvio ad atti interni depositati presso il servizio, occultamento dati, uso di codici identificativi).
Nel regime di pubblicità delle deliberazioni comunali e degli altri atti amministrativi comunali vanno rispettati i principi di pertinenza e non eccedenza al fine di selezionare i dati personali, specie se sensibili, la cui inclusione negli atti comunali da pubblicare sia realmente necessaria per le finalità conseguite dai singoli provvedimenti. In qualsiasi caso è fatto salvo il divieto di diffondere dati idonei a rilevare lo stato di salute.
L'affissione all'albo pretorio costituisce una forma di comunicazione o diffusione di dati a privati che il D. Lgs. 196/2003 consente solo se prevista da norma di legge o di regolamento.

Articolo 17 – Le sanzioni

L'inosservanza delle disposizioni di cui al Decreto Legislativo 196/2003 comporta sanzioni sia penali, sia amministrative:
L'omessa o inidonea informativa all'interessato (art. 161) – Sanzione da 3.000,00 a 18.000,00 Euro;
Assenza informativa nei casi di dati sensibili o giudiziari o in caso di trattamenti che presentano rischi specifici o di maggiore rilevanza del pregiudizio – Sanzione da 5.000,00 a 30.000,00 Euro (la somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore);
Omessa o incompleta notificazione al Garante Privacy (art. 163) – Sanzione da 10.000,00 a 60.000,00 Euro;
I danni causati dal trattamento di dati personali originano una responsabilità civile aggravata ai sensi dell'art. 2050 del C.C.;
Omessa informazione o esibizione di documenti richiesti dal Garante Privacy (art. 164) – Sanzione da 4.000,00 a 24.000,00 Euro;
Trattamento illecito di dati personali (art. 167) – Reclusione da 6 mesi a 3 anni. Possibile estinguere il reato ex art. 169, pagando una somma di denaro se ci si regolarizza entro il termine prescritto (non più di 6 mesi);
Falsità nelle dichiarazioni notificazioni al Garante Privacy (art. 168) – Sanzione penale, reclusione da 6 mesi a 3 anni;
Omessa adozione di misure necessarie alla sicurezza dei dati (art. 169) – Arresto fino a 2 anni o sanzione amministrativa, pagamento di una somma da 10.000,00 a 50.000,00 Euro.

Articolo 18 – Disposizioni finali

Per quanto non previsto dal presente Regolamento si applicano le disposizioni di cui alla normativa vigente in materia di trattamento dei dati personali, nonché dei provvedimenti del Garante.

Articolo 19 – Entrata in vigore

Il presente regolamento entra in vigore 15 giorni dopo la pubblicazione all'Albo Pretorio del Comune.

COMUNE di MALETTO
Titolare del Trattamento dei dati
f.to IL SINDACO
Giuseppe DE LUCA