

Il Codice della Privacy nella P.A.

Comune di Capoterra (CA)
4-5 ottobre 2010

Relatore: *Massimo Farina*
www.massimofarina.it

Struttura del Codice

si compone di 3 parti:

- I – Disposizioni Generali
- II – Disposizioni Relative a Settori Specifici
- III – Tutela dell'Interessato e Sanzioni

.... e di 3 allegati

- A – Codici Deontologici (storici, statistici, giornalisti)
- B – Disciplinare Tecnico
- C – Trattamenti in ambito giudiziario ...

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

Le definizioni del Codice Privacy (art. 4)

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

I Soggetti

“Titolare” (del trattamento)

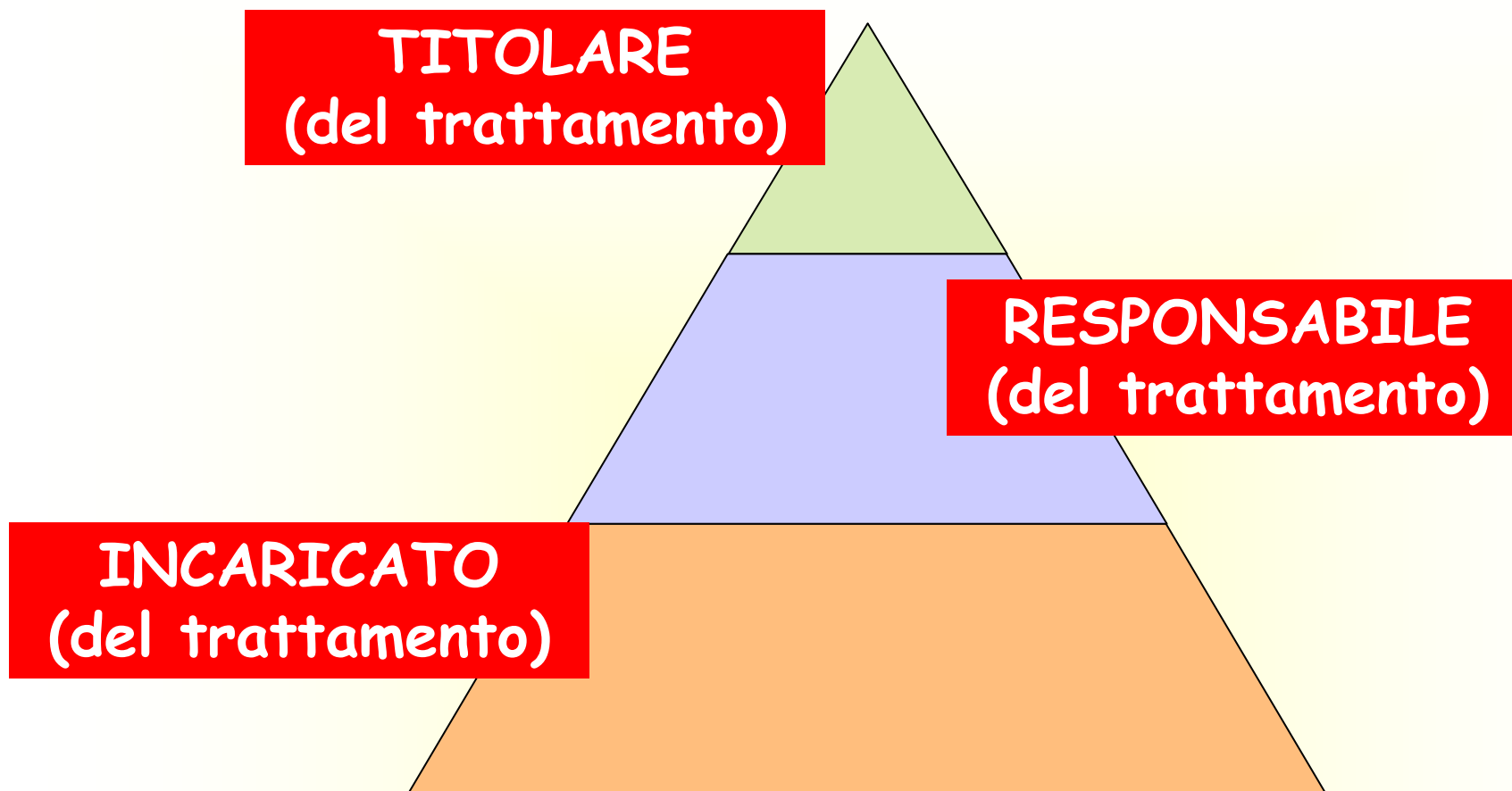
“la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il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

“Responsabile” (del trattamento)

“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” (del trattamento)

“le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile”



TIPICA ORGANIZZAZIONE PER IL TRATTAMENTO DEI DATI PERSONALI

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

Tipologia di Dati

DATI PERSONALI

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 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 [...] informazioni 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 [...]

TRATTAMENTO DEI DATI

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

I Principi del Codice Privacy

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

PRINCIPIO DI FINALITA'

(ART. 11, COMMA 1, LETTERA B)

**I DATI PERSONALI OGGETTO DI TRATTAMENTO
DEVONO ESSERE RACCOLTI E REGISTRATI PER
DETERMINATI SCOPI. CIÒ VUOL DIRE CHE OGNI
ATTIVITÀ È CONSENTITA SOLO SE È ANCORATA
AD UNA FINALITÀ OVVERO SE INERENTE CON
L'ATTIVITÀ PRESTATATA**

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

PRINCIPIO DI NECESSITA'

(ART. 3)

I SISTEMI INFORMATIVI E I PROGRAMMI INFORMATICI SONO CONFIGURATI RIDUCENDO AL MINIMO L'UTILIZZAZIONE DEI DATI PERSONALI E DEI DATI IDENTIFICATIVI, IN MODO DA ESCLUDERNE IL TRATTAMENTO QUANDO LE FINALITÀ PERSEGUITE NEI SINGOLI CASI POSSONO ESSERE REALIZZATE MEDIANTE, RISPETTIVAMENTE, DATI ANONIMI OD OPPORTUNE MODALITÀ CHE PERMETTANO DI IDENTIFICARE L'INTERESSATO SOLO IN CASO DI NECESSITÀ.

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

**PRINCIPIO DI
PROPORZIONALITA'**
(ART. 11, COMMA 1, LETTERA D)

**I DATI PERSONALI OGGETTO DI TRATTAMENTO
DEVONO ESSERE PERTINENTI, COMPLETI E NON
ECCEDENTI RISPETTO ALLE FINALITÀ PER LE
QUALI SONO RACCOLTI O SUCCESSIVAMENTE
TRATTATI**

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

PRINCIPIO DI INDISPENSABILITA'

(ART. 22, COMMA 3)

I SOGGETTI PUBBLICI POSSONO TRATTARE SOLO I DATI SENSIBILI E GIUDIZIARI INDISPENSABILI PER SVOLGERE ATTIVITÀ ISTITUZIONALI CHE NON POSSONO ESSERE ADEMPIUTE, CASO PER CASO, MEDIANTE IL TRATTAMENTO DI DATI ANONIMI O DI DATI PERSONALI DI NATURA DIVERSA

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

I Dati personali trattati nel Comune

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

Dati generalmente trattati nel COMUNE

Dati relativi al Personale:

- Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune.
- Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attività relativa al riconoscimento di benefici connessi all'invalidità civile per il personale e all'invalidità derivante da cause di servizio, nonché da riconoscimento di inabilità a svolgere attività lavorativa.

Servizi demografici:

- Anagrafe: gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero.
- Stato civile: Attività di gestione dei registri di stato civile.
- Elettorale: attività relativa all'elettorato attivo e passivo.
- Elettorale: attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio.
- Elettorale: attività relativa alla tenuta dell'elenco dei giudici popolari.
- Leva: attività relativa alla tenuta del registro degli obiettori di coscienza.
- Leva: attività relativa alla tenuta delle liste di leva e dei registri matricolari.

Dati generalmente trattati nel COMUNE

Servizi sociali:

- Attività relativa all'assistenza domiciliare.
- Attività relativa all'assistenza scolastica ai portatori di handicap o con disagio psico-sociale.
- Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc. .
- Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale
- Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti audiolesi, non vedenti, pluriminorati o gravi disabili o con disagi psico-sociali).
- Attività relativa all'integrazione sociale ed all'istruzione del portatore di handicap e di altri soggetti che versano in condizioni di disagio sociale (centro diurno, centro socio educativo, ludoteca, etc.).
- Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto.
- Attività relativa alla prevenzione ed al sostegno alle persone tossicodipendenti ed alle loro famiglie tramite centri di ascolto (per sostegno) e centri documentali (per prevenzione).
- Attività relativa ai servizi di sostegno e sostituzione al nucleo familiare e alle pratiche di affidamento e di adozione dei minori.
- Attività relativa ai trattamenti sanitari obbligatori ed all'assistenza sanitaria obbligatoria.
- Attività relative alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario.

Dati generalmente trattati nel COMUNE

Istruzione e cultura:

- Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie.
- Attività di formazione ed in favore del diritto allo studio.
- Gestione delle biblioteche e dei centri di documentazione.

Polizia municipale:

- Attività relativa all'infortunistica stradale.
- Gestione delle procedure sanzionatorie.
- Attività di polizia annonaria, commerciale ed amministrativa.
- Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria.
- Attività relativa al rilascio di permessi per invalidi.

Area Legale:

- Attività relative alla consulenza giuridica, nonché al patrocinio ed alla difesa in giudizio dell'amministrazione nonché alla consulenza e copertura assicurativa in caso di responsabilità civile verso terzi dell'amministrazione.

Dati generalmente trattati nel COMUNE

Ulteriori Trattamenti:

- Politiche del lavoro: Gestione delle attività relative all'incontro domanda/offerta di lavoro, comprese quelle relative alla formazione professionale.
- Gestione dei dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni.
- Conferimento di onorificenze e di ricompense.
- Tenuta di albi comunali di Associazioni ed Organizzazioni di Volontariato.
- Trattamenti per scopi statistici effettuati dall'Ufficio comunale di Statistica.
- ecc

I SOGGETTI "PRIVACY" NELL'ENTE LOCALE

➤ IL TITOLARE DEL TRATTAMENTO

È Colui che ha la legale rappresentanza pro tempore dell'Ente locale: **il Sindaco**.

Compiti:

- Decide in ordine alle finalità e alle modalità del trattamento dei dati personali, nonché ai profili della sicurezza;
- Stabilisce e specifica le linee strategiche per quanto attiene l'applicazione della legge e definisce l'organizzazione della privacy nella struttura.

Compiti esclusivi:

- Notificazione al Garante;
- Nomina dei responsabili;
- Nomina degli incaricati se non è designato alcun responsabile;
- Controllo e verifica dell'operato dei responsabili;
- Cessazione del trattamento dei dati.

Responsabilità:

- Penale,
- civile,
- amministrativa

I SOGGETTI "PRIVACY" NELL'ENTE LOCALE

➤ IL RESPONSABILE DEL TRATTAMENTO

È colui che sovrintende al trattamento dei dati per il proprio ambito di attribuzioni, funzioni e compiti:
p.es. **Dirigente e/o Funzionario**.
È nominato dal titolare con atto formale.

Compiti (analiticamente specificati nell'atto di nomina del titolare):

- Nomina gli incaricati del trattamento dei dati;
- Impartisce disposizioni organizzative e operative per il corretto e lecito trattamento dei dati e per la sicurezza degli stessi;
- Propone al titolare la nomina di soggetti esterni, quali responsabili del trattamento dei dati;
- Nomina i soggetti esterni quali incaricati del trattamento dei dati.

Responsabilità (limitatamente ai compiti e alle funzioni):

- Penale,
- civile,
- amministrativa

I SOGGETTI "PRIVACY" NELL'ENTE LOCALE

➤ L'INCARICATO DEL TRATTAMENTO

È ogni dipendente/collaboratore che nell'esercizio delle mansioni assegnate tratta dati personali: p. es. l'impiegato dell'ufficio anagrafe o protocollo
È nominato dal titolare con atto formale contrattuale e di nomina.

Compiti (analiticamente specificati nel decreto di nomina del responsabile):

- Tratta i dati nel rispetto dei principi di legittimità, pertinenza e stretta necessità, ponendo particolare attenzione all'informativa ai cittadini e alle operazioni di comunicazione e diffusione dei dati;
- Osserva le disposizioni organizzative e operative impartite;
- Adotta le misura e gli interventi per la sicurezza del trattamento dei dati.

Responsabilità (limitatamente alla sua autonomia gestionale e alle funzioni svolte):

- Penale,
- civile,
- amministrativa

I SOGGETTI "PRIVACY" NELL'ENTE LOCALE

➤ RESPONSABILI E INCARICATI ESTERNI

Soggetti che trattano dati di cui è titolare l'Ente locale in occasione dello svolgimento di determinate attività tramite convenzione, concessioni, ecc.

Sono nominati dal titolare, o dal Responsabile interno, con atto formale.

Compiti e Responsabilità:

Assume rispettivamente gli stessi compiti e responsabilità degli incaricati e dei responsabili interni, in relazione alle funzioni svolte.

I SOGGETTI "PRIVACY" NELL'ENTE LOCALE

➤ AMMINISTRATORE DI SISTEMA

Soggetto che vigila sul corretto utilizzo dei sistemi informatici dell'Ente.

Compiti:

L'amministratore di sistema non è semplicemente il manutentore della struttura informatica ma è il "garante informatico" della protezione delle informazioni personali unitamente al titolare.

Responsabilità (limitatamente ai compiti e alle funzioni):

- Penale,
- civile,
- amministrativa

NOVITÀ:

- Figura (re)introdotta con Provvedimento a carattere generale del Garante Privacy - 27 novembre 2008
- Il termine per la prima nomina è scaduto il 15 dicembre 2009

BREVE APPROFONDIMENTO SUGLI AMMINISTRATORI DI SISTEMA

Prov. Gen. 27 novembre 2008

(G.U. n. 300 del 24 dicembre 2008 - modificato il 25 giugno 2009)

AMMINISTRATORI DI SISTEMA

Soggetti che vigilano sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione.

L'amministratore di sistema non è semplicemente il manutentore della struttura informatica ma è il "garante informatico" della protezione delle informazioni personali unitamente al titolare.

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

AMMINISTRATORE DI SISTEMA

Non è una figura nuova nell'ordinamento italiano.
Esisteva già nel Regolamento attuativo (DPR 318/1999) della legge
675/1996.

Esistevano due figure:

1. il preposto alla custodia della parola chiave
2. l'amministratore di sistema. (abrogato dall'art. 183, D.Lgs. n. 196/03)

AMMINISTRATORE DI SISTEMA

1. Deve trattarsi di un soggetto affidabile.

"...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".

2. Si deve procedere alla designazione individuale ovvero occorre predisporre apposita nomina scritta con il profilo di operatività corrispondente al profilo di autorizzazione assegnato.

AMMINISTRATORE DI SISTEMA

3. Devono essere resi noti al pubblico e ai lavoratori gli estremi identificativi dell'amministratore di sistema tramite menzione nel DPS.

“...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) 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”.

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

AMMINISTRATORE DI SISTEMA

4 Si deve procedere alla verifica delle relative attività mediante controllo almeno annuale.

5 Devono essere adottati sistemi idonei alla registrazione degli accessi.

“....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”.

LA ROTTAMAZIONE DI APPARECCHIATURE ELETTRICHE ED ELETTRONICHE

Comunicato stampa - 05 dicembre 2008

Misure tecniche preventive

È bene proteggere i file usando una **password di cifratura**, oppure memorizzare i dati su hard disk o su altri supporti magnetici usando sistemi di **cifratura automatica** al momento della scrittura.

Misure tecniche di cancellazione sicura

La cancellazione sicura delle informazioni su disco fisso o su altri supporti magnetici è ottenibile con **programmi informatici di "riscrittura"** che provvedono - una volta che l'utente abbia eliminato dei file dall'unità disco con i normali strumenti previsti dai sistemi operativi (ad es., con l'uso del "cestino" o con comandi di cancellazione) - a scrivere ripetutamente nelle aree vuote del disco. Si possono anche utilizzare sistemi di formattazione a basso livello degli hard disk o di "demagnetizzazione", in grado di garantire la cancellazione rapida delle informazioni.

Smaltimento di rifiuti elettrici ed elettronici

Per la distruzione degli hard disk e di supporti magnetici non riscrivibili, come cd rom e dvd, è consigliabile l'utilizzo di sistemi di punzonatura o deformazione meccanica o di demagnetizzazione ad alta intensità o di vera e propria distruzione fisica.

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

Gli Adempimenti

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

I PRINCIPALI ADEMPIMENTI

➤ ADEMPIMENTI VERSO L'AUTORITÀ GARANTE

Notificazione

Autorizzazione

➤ ADEMPIMENTI VERSO GLI INTERESSATI

Informativa

Richiesta di consenso

➤ ADEMPIMENTI INTERNI (O ORGANIZZATIVI)

Misure minime di sicurezza

Notificazione

Quando si notifica ?

Nei casi elencati nell'art. 37 Codice della Privacy

- 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 diffuse, 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;
[.....]

Notificazione

[.....]

- 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.

1-bis. La notificazione relativa al trattamento dei dati di cui al comma 1 non è dovuta se relativa all'attività dei medici di famiglia e dei pediatri di libera scelta, in quanto tale funzione è tipica del loro rapporto professionale con il Servizio sanitario nazionale.

[.....]

Notificazione

[.....]

2. Il Garante può **individuare altri trattamenti** suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla Gazzetta Ufficiale della Repubblica italiana il Garante **può anche individuare**, nell'ambito dei trattamenti di cui al comma 1, eventuali **trattamenti** non suscettibili di recare detto pregiudizio e pertanto **sottratti all'obbligo di notificazione**.
3. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.
4. Il Garante inserisce le notificazioni ricevute in un **registro dei trattamenti** accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

[.....]

Notificazione

Come si notifica?

Art. 38. Modalità di notificazione [II] La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione. [Tramite il sito www.garanteprivacy.it]

Notificazione

Quante volte si notifica?

Art. 38. Modalità di notificazione [IV] Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.

Sanzione per omessa notificazione?

Art. 163. Omessa o incompleta notificazione
[...] sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione. (Sanzione oggi raddoppiata ex D.L. 207/2008 “Decreto Milleproroghe”)

Un caso pratico: Omessa Notificazione

13 settembre 2007

“Ordinanza ingiunzione nei confronti del Comune di Moncalieri”

L'Autorità Garante:

ORDINA

al Comune di Moncalieri, con sede in Moncalieri (TO) Piazza Vittorio Emanuele II, in persona del legale rappresentante *pro-tempore*, di pagare **la somma di euro 10.000,00** (diecimila) a titolo di sanzione amministrativa pecuniaria per la violazione dell'art. 163 del Codice, indicata in motivazione;

DISPONE

la **pubblicazione** a cura dell'Ufficio della presente ordinanza-ingiunzione a titolo di sanzione amministrativa accessoria prevista dall'art. 163 del Codice, per estratto e per una sola volta, **sulle testate giornalistiche "La Stampa" e "Il Giornale nuovo del Piemonte"**;

Comportamento contestato:

Trattamento ex art. 37, comma 1, lett. a) del Codice, da epoca anteriore al 1° gennaio 2004 (**trattamento di dati biometrici**);

Notificazione eseguita in data 27 marzo 2006 (oltre il termine previsto dall'art. 181, comma 1, lett. c) del Codice (30 aprile 2004)

Autorizzazione



prevista per tutti i Titolari che trattano dati sensibili e giudiziari

DISCIPLINA
PARTICOLARE
PER LA P.A.

Art. 18, comma 2, Codice Privacy: i soggetti pubblici possono trattare qualunque tipologia di informazioni personali purchè ciò avvenga nello svolgimento di funzioni istituzionali (cd. principio di finalità) attribuite dalla Legge, osservando i presupposti e i limiti stabiliti dal Codice, dalla Legge e dai Regolamenti, anche in relazione alla natura dei dati trattati.

La fonte legislativa di base che definisce di interesse pubblico le attività istituzionali svolte dai Comuni è il D.lgs. 196/03

Artt. 20, comma 2, e 21, comma 2, Codice Privacy: se una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e giudiziari trattabili ed i tipi di operazioni su questi eseguibili, il trattamento è consentito solo in riferimento a quei 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.

L'individuazione deve avvenire mediante l'adozione di un atto Regolamentare conforme al parere adottato dal Garante nel [settembre del 2005](#)

Autorizzazione



DISCIPLINA PARTICOLARE PER LA P.A.

L'art. 20, comma 2, Codice Privacy, prevede che il Regolamento Comunale per i dati sensibili va adottato nel rispetto dei principi di cui all'art. 22 del medesimo Codice, in particolare, assicurando che i soggetti pubblici:

- a)** trattino i soli dati sensibili e giudiziari indispensabili per le relative attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa;
- b)** raccolgano detti dati, di regola, presso l'interessato;
- c)** verifichino periodicamente l'esattezza, l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza ed indispensabilità rispetto alle finalità perseguite nei singoli casi;
- d)** trattino i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi;
- e)** conservino i dati idonei a rivelare lo stato di salute e la vita sessuale separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo;

Tenuto conto dell'altissimo numero di soggetti interessati, il legislatore ha previsto le “Autorizzazioni Generali” concesse a determinate categorie di titolari o di trattamenti

- **Autorizzazione generale n. 1/2009 del 16 dicembre 2009**
“Trattamento dei dati sensibili nei rapporti di lavoro”
- **Autorizzazione generale n. 2/2009 del 16 dicembre 2009**
“Trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale”
- **Autorizzazione generale n. 3/2009 del 16 dicembre 2009**
“Trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni”
- **Autorizzazione generale n. 4/2009 del 16 dicembre 2009**
“Trattamento dei dati sensibili da parte dei liberi professionisti”
- **Autorizzazione generale n. 5/2009 del 16 dicembre 2009**
“Trattamento dei dati sensibili da parte di diverse categorie di titolari”
- **Autorizzazione generale n. 6/2009 del 16 dicembre 2009**
“Trattamento dei dati sensibili da parte degli investigatori privati”
- **Autorizzazione generale n. 7/2009 del 16 dicembre 2009**
“Trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici”

INFORMATIVA

Art. 13. Informativa.

L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati **oralmente o per iscritto** circa:

- le finalità e le modalità del trattamento;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti ai quali i dati possono essere comunicati;
- i soggetti, incaricati o responsabili, che possono venirne a conoscenza
- l'ambito di diffusione;
- i diritti riconosciuti dalla legge;
- le generalità del titolare e del responsabile del trattamento dei dati o, se designato, del responsabile per l'esercizio dei diritti dell'interessato.
- nel caso di trattamento di dati sensibili o giudiziari, ai sensi dell'art. 22, comma 2, del Codice, espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento.

INFORMATIVA

- può essere in forma **orale o scritta**: è tuttavia consigliabile la forma scritta quale prova dell'avvenuta comunicazione;
- se è resa per iscritto, mediante lettere moduli predisposti dalla P.A. o dal singolo ufficio (oltre all'informativa specifica relativa ai procedimenti e/o a quella contenuta nei moduli relativi a istanze o dichiarazioni sostitutive, si consiglia ed è opportuno **redigere e affiggere in luogo accessibile al pubblico** un'informativa generale relativa all'attività del Servizio).
- **non può essere generica** o rinviare a finalità istituzionali non ben precisate ma deve essere completa ed analitica al fine di consentire all'interessato di conoscere i vari aspetti del trattamento;
- deve contenere le indicazioni necessarie a consentire l'identificazione e la possibilità di mettersi in contatto con il Titolare e/o il Responsabile.

Consenso dell'interessato: in generale

DEFINIZIONE: libera manifestazione della volontà dell'interessato con cui egli accetta espressamente un determinato trattamento dei propri dati personali, previa informativa da chi gestisce i dati.

I REQUISITI DEL CONSENSO

- **INFORMATO**: è invalido il consenso non preceduto da informativa (Garante Provv. 28 maggio 1997)
- **ESPRESSO**: non può essere implicito, né per comportamenti concludenti (Garante Provv. 25 dicembre 1998)
- **LIBERO**: non costretto e non condizionato (Garante Provv. 28 maggio 1997)
- **SPECIFICO**: è invalido se generico
- **DOCUMENTATO PER ISCRITTO**: annotato, trascritto, riportato dal titolare o dal responsabile o da un incaricato del trattamento su un registro o un atto o un verbale. In caso di dati sensibili occorre il consenso rilasciato per iscritto dall'interessato

Consenso dell'interessato nella P.A.

I soggetti pubblici, tra cui il Comune, **non devono raccogliere il consenso** degli interessati, poiché il Codice consente loro di effettuare trattamenti di dati personali soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti da leggi e da regolamenti.

ALTRI CASI DI ESCLUSIONE (Art. 24):

- a) trattamento effettuato per adempiere a prescrizioni di legge/regolamenti/norme CE;
- b) trattamento necessario per eseguire un contratto di cui sia parte l'interessato o, prima della conclusione del contratto, per adempiere a specifiche richieste dell'interessato;
- c) trattamento di dati provenienti da pubblici registri, elenchi o atti di dominio pubblico;
- d) trattamento necessario per la salvaguardia della vita/incolumità fisica di un terzo;
- e) trattamento necessario per lo svolgimento di investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria;
- f) trattamento necessario, nei casi individuati dal Garante, per perseguire un interesse legittimo del titolare o del terzo destinatario dei dati;
- g) trattamento effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, ove il trattamento abbia ad oggetto dati degli aderenti o di soggetti che abbiano con l'ente dei contatti regolari;
- h) il trattamento necessario, nel rispetto dei rispettivi codici deontologici, per scopi di archiviazione scientifica, statistica o storica.

Disciplinare Tecnico "Misure Minime di Sicurezza".



**MISURE MINIME
DI SICUREZZA**

**MISURE IDONEE
DI SICUREZZA**

CARATTERISTICHE DELLE CREDENZIALI DI AUTENTICAZIONE	<ol style="list-style-type: none">1. Lunghezza minima della password di 8 caratteri,2. non riconducibile al soggetto
GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE	<ol style="list-style-type: none">1. Modifica dopo il primo utilizzo, ogni 6 o 3 mesi a seconda dei dati trattati2. Disattivazione in caso di non uso per almeno 6 mesi o di perdita della qualità che permette l'accesso ai dati3. Garanzia della disponibilità dei dati o degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che goda delle credenziali di autenticazione

SISTEMA DI AUTORIZZAZIONE	Verifica almeno annuale delle condizioni per l'autorizzazione
PROTEZIONE CONTRO IL RISCHIO DI INTRUSIONE	Attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
AGGIORNAMENTI PERIODICI DEI PROGRAMMI PER ELABORATORE	<ul style="list-style-type: none">•Almeno annuale per dati comuni•Almeno semestrale per dati sensibili e/o giudiziari

BACK UP	salvataggio dei dati con frequenza almeno settimanale
DISASTER RECOVERY	Ripristino entro il termine massimo di una settimana

“Misure minime di sicurezza” VS “Misure idonee di sicurezza”

È NECESSARIO PRESTARE ATTENZIONE ALLA DISTINZIONE TRA MISURE MINIME DI SICUREZZA E MISURE IDONEE DI SICUREZZA

art. 4 comma 3 del D.Lgs. 196/03: “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”.

MISURE MINIME

MISURE IDONEE

NESSUNA DEFINIZIONE NORMATIVA: sono individuabili sulla base delle soluzioni tecniche concretamente disponibili sul mercato, mentre le misure minime sono puntualmente individuate dalla legge (in particolare dall'allegato B)”.

“Misure minime di sicurezza” VS “Misure idonee di sicurezza”

**CONSEGUENZE DIVERSE PER IL MANCATO RISPETTO DELLE MISURE MINIME
DI SICUREZZA E DELLE MISURE IDONEE DI SICUREZZA**

Responsabilità di tipo amministrativo e penale

MISURE MINIME

MISURE IDONEE

Responsabilità Civile ex art. 2050 c.c.

Il DPS

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

➤ l'elenco dei trattamenti

➤ i compiti e le responsabilità dei soggetti incaricati al trattamento

➤ l'analisi dei rischi con l'indicazione delle misure che sono adottate al fine di garantire l'integrità e la disponibilità dei dati

➤ la protezione delle aree e dei locali in relazione alla loro custodia ed accessibilità

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

➤ l'analisi dei rischi con l'individuazione delle modalità che possono essere poste a favore del ripristino della disponibilità dei dati qualora si verificano episodi di distruzione o danneggiamento

➤ gli interventi formativi in tema di analisi dei rischi che incombono sui dati

➤ i criteri per l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura (outsourcing)

➤ criteri adottati per la separazione dei dati sensibili da quelli comuni.

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

➤ Protezione contro l'accesso abusivo con strumenti hardware e software

➤ Attenta gestione dei supporti magnetici rimovibili

➤ Ripristino della disponibilità dei dati entro sette giorni

➤ Particolari misure fisiche e logiche di protezione per i dati genetici – cifratura –

Internet e Posta Elettronica

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it



**REGOLE
PARTICOLARI**

Linee guida del Garante per Posta
Elettronica e Internet

Deliberazione 1 marzo 2007 n. 13
(Gazzetta Ufficiale n. 58 del 10 marzo 2007)

Linee guida del Garante in materia
di trattamento di dati personali per
finalità di pubblicazione e diffusione
di atti e documenti di enti locali
(Gazzetta Ufficiale n. 120 del 25 maggio 2007)

Direttiva (Brunetta) n. 2/2009
Utilizzo di internet e della casella di
posta elettronica istituzionale sul
luogo di lavoro (26 maggio 2009)

Linee guida del Garante
per Posta Elettronica e Internet
Deliberazione 1 marzo 2007 n. 13
(Gazzetta Ufficiale n. 58 del 10 marzo 2007)

- Adozione e pubblicizzazione di un disciplinare interno
- Adozione di misure di tipo tecnologico per l'utilizzo di internet e per la posta elettronica
- Attività di controllo

Adozione e pubblicizzazione di un disciplinare interno

- elencazione dei comportamenti non tollerati rispetto alla "navigazione" in Internet (ad es. il *download* di *software* o di *file* musicali), oppure alla tenuta di file nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es. fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es. le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);

[.....]

Adozione e pubblicizzazione di un disciplinare interno

[.....]

•se, e in quale misura, il Comune si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime, specifiche e non generiche, per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);

•quali conseguenze, anche di tipo disciplinare, il Comune si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;

•le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;

•se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato.

Adozione di misure di tipo tecnologico per l'utilizzo di internet

- individuare categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurare i sistemi o l'utilizzo di filtri che prevengano determinate operazioni, reputate inconferenti con l'attività lavorativa, quali l' upload o l'accesso a determinati siti (inseriti in una sorta di black list) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattare i dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es. con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- conservare i dati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza.

Adozione di misure di tipo tecnologico per l'utilizzo della posta elettronica

- valutare se rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori;
- valutare se attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;
- predisporre apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.

Attività di controllo

- L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.
- Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.
- Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.
- Non sono legittimi controlli prolungati, costanti o indiscriminati.
- I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Attività di controllo: Divieti!!!

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso.

Linee guida del Garante in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali (Gazzetta Ufficiale n. 120 del 25 maggio 2007)

- Predisposizione di un Regolamento Comunale ad hoc sull'albo pretorio virtuale.
- Prima di pubblicare gli atti, renderli accessibili a terzi o metterli in rete, l'ente locale deve valutare se le finalità di trasparenza possano essere perseguite senza divulgare dati personali o attraverso modalità che permettano di identificare gli interessati solo se necessario.

Non c'è equivalenza tra pubblicabilità sull'albo pretorio e sul sito internet del Comune (o della Provincia).



Neccessità di una fonte (legislativa o regolamentare), che attui contemporaneamente i principi della trasparenza e della riservatezza.

La pubblicazione del documento all'albo pretorio ha una scadenza di 15 giorni; deve avvenire altrettanto sull'albo virtuale con previsione in una fonte normativa o regolamentare

Con il regolamento devono essere dettagliati anche i diversi piani di accesso alle informazioni pubblicate sul web: atti conoscibili da chiunque o atti destinati soltanto ad alcune categorie di persone (accesso con username e password).

RISPETTO DEI PRINCIPI DI PERTINENZA, NON ECCEDENZIA E INDISPENSABILITÀ

CIOÈ

- I funzionari pubblici devono selezionare le informazioni necessarie da quelle non necessarie ed eliminare queste ultime dalla parte degli atti in cui si descrivono i presupposti di fatto.
- Negli atti devono comparire solo dati pertinenti e non eccedenti rispetto alle finalità che l'ente intende raggiungere. I dati sensibili e giudiziari possono essere diffusi solo se realmente indispensabili e se l'ente abbia adottato il regolamento previsto dal codice sull'uso di questi dati. È sempre vietato diffondere informazioni sulla salute.

Privacy e Accesso

Tutela della riservatezza
(D.lgs. 196/03)

FINALITÀ
PERSEGUITE

Tutela della personalità

Oggetto
di tutela

**dati personali, in se e per
se considerati, a
prescindere dal supporto
sul quale sono contenuti**

Garanzia del diritto d'accesso
(capo V della Legge n. 241/1990)

FINALITÀ
PERSEGUITE

**Partecipazione al procedimento
amministrativo**

Oggetto
di tutela

**atti e documenti
che fanno parte di
un procedimento
amministrativo**

I PRINCIPI

PRINCIPIO DI NECESSITÀ:

Prima di pubblicare gli atti, renderli accessibili a terzi o metterli in rete, l'ente locale deve valutare se le finalità di trasparenza possano essere perseguite senza divulgare dati personali o attraverso modalità che permettano di identificare gli interessati solo se necessario.

PRINCIPIO DI PERTINENZA E NON ECCEDENZIA:

Negli atti devono comparire solo dati pertinenti e non eccedenti rispetto alle finalità che l'ente intende raggiungere.

PRINCIPIO DI INDISPENSABILITÀ:

I dati sensibili e giudiziari possono essere diffusi solo se realmente indispensabili e se l'ente abbia adottato il regolamento previsto dal codice sull'uso di tali dati.

NOTA: divieto assoluto di diffusione di dati sanitari (articolo 22, comma 8, del codice della privacy)

PUBBLICAZIONE DI GRADUATORIE E DI PROVVEDIMENTI DELIBERATIVI

Non è obbligatoria la cifratura dei dati tale da rendere i documenti del tutto incomprensibili nella motivazione e nel dispositivo

Non è necessario esimersi dalla pubblicazione né trasformare gli atti in documenti vuoti dal contenuto non ricostruibile

LA REGOLA DA SEGUIRE:

Osservare i divieti specifici imposti dalla legge (ad es. il divieto di diffusione di dati sanitari) e ispirare la stesura dell'atto ai principi di pertinenza, non eccedenza e indispensabilità

Linee guida del Garante in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali

ESEMPIO

L'Ente autorizza, con proprio atto la costituzione in giudizio per difendersi da una richiesta di risarcimento del danno biologico



Si tratta di una delibera da diffondere mediante pubblicazione nell'albo pretorio, riguardante dati sanitari (danno biologico)



È obbligatorio selezionare le informazioni necessarie da quelle non necessarie ed eliminare queste ultime dalla parte degli atti in cui si descrivono i presupposti di fatto

nel testo della deliberazione si deve riportare che l'interessato (identificato nominativamente) ha promosso una causa per il risarcimento del danno

Motivazione per relationem: rinvio ad altri atti che contengono l'esplicitazione delle ragioni del provvedimento (conforme alla legge 241/1990)

Linee guida del Garante in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali

(Gazzetta Ufficiale n. 120 del 25 maggio 2007)

ALCUNI ESEMPI

SETTORE	REGOLE PER LA CONOSCIBILITÀ
Anagrafe	<ul style="list-style-type: none">• certificati residenza e stato di famiglia: a richiesta di chiunque• elenchi iscritti alle liste elettorali: a richiesta di P.A. per pubblica utilità
Stato civile	<ul style="list-style-type: none">• Estratti e certificati integrali: soltanto a richiesta degli interessati• Pubblicazioni matrimoniali: soltanto mediante affissione
Organizzazione	<ul style="list-style-type: none">• Organigramma, nominativo dirigenti, e-mail istituzionali: pubblicazione nel sito internet
Personale	<ul style="list-style-type: none">• Graduatoria dei concorsi: all'albo pretorio (nomi, risultati e punteggi)• Graduatorie sulla mobilità: soltanto con nomi e senza riferimento a dati sensibili

Linee guida del Garante in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali

(Gazzetta Ufficiale n. 120 del 25 maggio 2007)

ALCUNI ESEMPI

Ragioneria	Compensi di amministratori, dirigenti, consulenti: sul sito internet istituzionale
Ufficio tecnico	Permessi, sospensione lavori, immobili abusivi: pubblicazione in albo pretorio
Edilizia residenziale	Graduatoria di assegnazione alloggi: solo nomi e punteggi
Servizio sociale	Albo dei beneficiari: nominativi, data di nascita, norma sull'erogazione
Servizi educativi	Graduatorie asili nido: pubblicazione all'albo pretorio senza indicazione di punteggi abbinati a dati sensibili o di particolare delicatezza
Tributi	Elenchi nominativi: consultabili da chiunque per legge

Direttiva (Brunetta) n. 2/2009

Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro (26 maggio 2009)

REGOLE GENERALI

Dovere della Pubblica Amministrazione (datore di lavoro) per fini di sicurezza interna e sicurezza dei sistemi, di controllare l'uso di internet e della posta elettronica istituzionale

"Il dipendente non utilizza a fini privati materiale o attrezzature di cui dispone per ragioni di ufficio".
(decreto del Ministro per la funzione pubblica del 28 novembre 2000)

Il controllo deve rispettare il principio di proporzionalità: non può essere continuo, deve avere delle tempistiche, deve essere motivato da reali necessità e deve essere adeguato allo scopo da raggiungere

ESEMPIO



verificare se vi è stato indebito utilizzo della connessione ad internet da parte del dipendente attraverso il controllo degli accessi e dei tempi di connessione, **senza indagare sul contenuto dei siti visitati.**

Direttiva (Brunetta) n. 2/2009

Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro (26 maggio 2009)

CONDIZIONI PER IL CONTROLLO

- E' necessario informare le associazioni sindacali e i singoli lavoratori dell'esistenza di strumenti di controllo della rete e della posta elettronica
- divieto di installare strumenti per finalità di controllo a distanza dell'attività dei lavoratori (Legge 300/70);
- I lavoratori devono conoscere quali sono le attività consentite, a quali controlli sono sottoposti, le modalità del trattamento dei dati e in quali sanzioni possono incorrere nel caso di abusi (Linee guida del Garante per posta elettronica e internet, 10 marzo 2007)
- L'amministrazione può limitare l'accesso a internet dei dipendenti ai soli siti considerati correlati all'attività lavorativa e vietare quindi la visione di siti ad es. "hard", giochi on line etc; limitare il download e l'upload di file e

Direttiva (Brunetta) n. 2/2009

Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro (26 maggio 2009)

ECCEZIONE ALL'USO DEGLI STRUMENTI DI LAVORO PER ESCLUSIVE FINALITÀ COLLEGATE ALL'ATTIVITÀ LAVORATIVA

"Tuttavia, l'utilizzo di Internet per svolgere attività che non rientrano tra i compiti istituzionali potrebbe essere regolamentato e, quindi, consentito ai dipendenti per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio, per effettuare adempimenti online nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi). Tale modalità, purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni, avrebbe, inoltre, il vantaggio di contribuire a ridurre gli spostamenti delle persone e gli oneri logistici e di personale per l'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi"

Responsabilità, Sanzioni e Tutela

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

IL CODICE PREVEDE TRE TIPI DI RESPONSABILITÀ:

➤ AMMINISTRATIVA

Artt. 161- 166

➤ CIVILE

Art. 15

➤ PENALE

Artt. 167- 172

TITOLO III
Sanzioni.
Capo I - Violazioni amministrative
Artt. 161-166

L'organo competente ad irrogare le sanzioni amministrative è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni.

art. 161 – OMESSA O INIDONEA INFORMATIVA ALL'INTERESSATO

DA €. 3.000 a 18.000

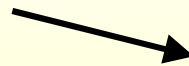
SE RIGUARDA DATI COMUNI

DA €. 5.000 a 30.000

SE RIGUARDA DATI SENSIBILI

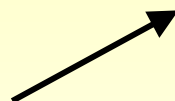
**MOLTIPLICABILE PER TRE IN RELAZIONE ALLE CONDIZIONI
ECONOMICHE DEL CONTRAVVENTORE**

art. 163 – Omessa o
incompleta notificazione al
garante



da €. 10.000 a 60.000

Art. 164 – Omesso invio di
informazioni o documenti
richiesti dal garante



da €. 4.000 a 24.000

RESPONSABILITA' CIVILE

Art. 15. Danni cagionati per effetto del trattamento.

Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

Art. 2050 c.c.: Responsabilità per l'esercizio di attività pericolose.

Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno

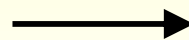
TITOLO III
Sanzioni.
Capo II – Illeciti Penali
Artt. 167-172

**Art. 167 – TRATTAMENTO
ILLECITO DI DATI PERSONALI**



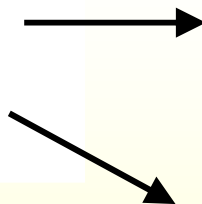
1. se dal fatto deriva documento, reclusione da sei a diciotto mesi
2. se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

**Art. 168 – FALSITÀ NELLE
DICHIARAZIONI E NOTIFICAZIONI
AL GARANTE**



salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni

**Art. 169 – OMISSIONE DI
ADOZIONE DELLE MISURE
MINIME DI SICUREZZA**

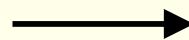


arresto sino a due anni o
ammenda da €. 10.000 a
50.000.

RAVVEDIMENTO OPEROSO

All'autore è impartita una prescrizione fissando un termine per la regolarizzazione. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione.

**Art. 170 – INOSSERVANZA DEI
PROVVEDIMENTI DEL GARANTE**



reclusione da tre mesi a due
anni

Forme di tutela

TUTELA GIURISDIZIONALE
GIUDICE ORDINARIO

TUTELA AMMINISTRATIVA
GARANTE

**Per il risarcimento dei danni
l'unica forma di tutela
ammessa è quella davanti al
Giudice Ordinario**

UN FATTO RECENTE

Art. 369 c.p.p.: istituto mediante il quale una persona viene avvertita di essere sottoposta a indagini preliminari, (fase processuale in cui si raccolgono elementi utili alla formulazione di una imputazione).

**Notificato un avviso di garanzia
al Responsabile dei sistemi informatici
del Comune di Milano**

REATI CONTESTATI

- omissione di controllo delle misure di sicurezza dei sistemi informativi
- false attestazioni rese al Garante in relazione all'adeguamento alle misure trascorso il termine prescritto dal medesimo Garante per la messa a norma

Art. 169. Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione [...] non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

ANTEFATTO



Un virus denominato Kamasutra infettò i PC del Comune di Milano

- **Sanzione pecuniaria di circa 70.000 euro per omissione di misure di sicurezza**
- **Assegnazione di un termine imposto per provvedere alla regolarizzazione degli antivirus: "ravvedimento".**

Scaduti i termini assegnati:

Il Responsabile dei sistemi informativi comunicò al Garante l'avvenuto adeguamento

Fine 2008:

l'Autorità Garante ha avviato una nuova attività di verifica presso il Comune di Milano dalla quale è emersa la presenza di antivirus sul 70% dei client presenti nei vari uffici

Privacy e Videosorveglianza

Comune di Capoterra 4 – 5 ottobre 2010

Massimo Farina - <http://www.massimofarina.it> - massimo@massimofarina.it

Privacy e Videosorveglianza

Provvedimento Generale del 8 aprile 2010

**Provvedimenti
precedenti**

DECALOGO SULLA VIDEOSORVEGLIANZA

Prov. Gen. 29 novembre 2000

Prov. Gen.
29 aprile 2004: integrativo del
“decalogo sulla
videosorveglianza”

Privacy e Videosorveglianza

PRINCIPIO DI FINALITÀ



chi installa telecamere deve perseguire finalità determinate e di propria pertinenza.

ESEMPI DI FINALITÀ

- 1) la sicurezza urbana, l'ordine e la sicurezza pubblica, la prevenzione, l'accertamento o la repressione dei reati;
- 2) la protezione della proprietà;
- 3) la rilevazione, prevenzione e controllo delle infrazioni da parte dei soggetti pubblici a ciò preposti dalla legge;
- 4) l'acquisizione di prove.

IERI

“Alcune amministrazioni comunali indicano indebitamente, come scopo della sorveglianza, finalità di sicurezza pubblica, prevenzione e accertamento dei reati che competono invece solo ad organi giudiziari o a forze armate o di polizia”

OGGI

“Recenti disposizioni legislative in materia di sicurezza (Decreto Legge antistupro del 23 febbraio 2009) hanno attribuito ai sindaci il compito di sovrintendere alla vigilanza ed all'adozione di atti che sono loro attribuiti dalla legge e dai regolamenti in materia di ordine e sicurezza pubblica, nonché allo svolgimento delle funzioni affidati ad essi dalla legge in materia di sicurezza e di polizia giudiziaria”

Privacy e Videosorveglianza: principi generali

PRINCIPIO DI LICEITÀ



l'attività di videosorveglianza deve essere conforme alle disposizioni dettate dal d.lgs. 196/03 per ciascuna categoria di titolari (pubblici o privati).

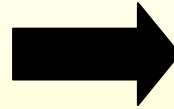
PRINCIPIO DI NECESSITÀ



Si possono riprendere persone identificabili solo se, per raggiungere gli scopi prefissati, non siano utilizzabili esclusivamente dati anonimi: ad esempio, nel caso di monitoraggio sul traffico, sono consentite soltanto riprese generali, che escludano la possibilità di rendere identificabili le persone.

Privacy e Videosorveglianza: principi generali

PRINCIPIO DI PERTINENZA E NON ECCEDENZIA



trattamento pertinente e non eccedente, rispetto alle finalità perseguite; ciò si concretizza, ad esempio, nella scelta delle modalità di ripresa e dislocazione delle telecamere (fisse o brandeggiabili, dotate o meno di zoom).

NOVITÀ

4.5. Utilizzo di web cam o camera-on-line a scopi promozionali-turistici o pubblicitari

Le attività di rilevazione di immagini a fini promozionali-turistici o pubblicitari, attraverso web cam devono avvenire con modalità che rendano non identificabili i soggetti ripresi. Ciò in considerazione delle peculiari modalità del trattamento, dalle quali deriva un concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete Internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle predette finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento.

Privacy e Videosorveglianza: l'INFORMATIVA

Tutti coloro che transitano nelle aree videocontrollate devono essere opportunamente informati della presenza di telecamere attraverso l'affissione di appositi cartelli chiaramente visibili ed esplicativi degli elementi previsti all'art. 13 del d.lgs. 196/03, anche quando il sistema di videosorveglianza è attivo in ORARIO NOTTURNO.

- **Il Provvedimento del 2010 introduce una nuova tipologia di informativa, per i soggetti privati che effettuano trattamenti di immagini con sistemi di videosorveglianza collegati con le forze di polizia;**
- **Rimane anche l'informativa già adottata con il Provvedimento del 2004**



Privacy e Videosorveglianza: L'INFORMATIVA

ESENZIONE

Art. 3.1.1. del Provv. 8 apr. 2010: sono esentati coloro che effettuano il trattamento, anche sotto forma di suoni e immagini, per le finalità indicate all'art. 53 del Codice della Privacy. Si tratta dei trattamenti svolti dalle forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. L'assenza dell'obbligo non significa, però, divieto; infatti, per i titolari dei predetti trattamenti è espressamente prevista la possibilità di *“rendere nota la rilevazione di immagini tramite impianti di videosorveglianza attraverso forme anche semplificate di informativa, che evidenzino, mediante l'apposizione nella cartellonistica di riferimenti grafici, simboli, diciture, l'utilizzo di tali sistemi per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati”*.

Privacy e Videosorveglianza: tempi di registrazione

TEMPO MASSIMO DI CONSERVAZIONE E REGISTRAZIONE DELLE IMMAGINI: 24 ORE

ECCEZIONI

•PER I COMUNI (sicurezza urbana): conservazione dei dati *“ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l’uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione”*.

•peculiari esigenze tecniche (mezzi di trasporto)

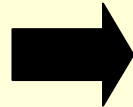
•particolare rischiosità dell'attività svolta dal titolare del trattamento (le banche, per le quali può risultare giustificata l’esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina)

É sempre obbligatoria la verifica preliminare del Garante nel caso di uso di sistemi intelligenti, dotati di *software* che permettono l’associazione di immagini a dati biometrici (es. “riconoscimento facciale”) ovvero in grado di riprendere e registrare automaticamente comportamenti o eventi anomali e segnalarli (“motion detection”).

ALTRE REGOLE PER I COMUNI CHE INSTALLANO SISTEMI DI VIDEOSORVEGLIENZA

FINALITÀ

- controllo del traffico cittadino, (Z.T.L.) telecontrollo ambientale
- presidio di monumenti o luoghi pubblici ecc....



limitare le possibilità di dettaglio sui tratti somatici delle persone quando le finalità possono essere raggiunte indipendentemente dall'utilizzo di tecniche particolarmente invasive dei diritti e della dignità dell'interessato (principio di necessità, di proporzionalità e di non eccedenza)

- I sistemi installati devono essere conformi alle misure di sicurezza previste dal Codice privacy per evitare i rischi di distruzione, perdita, anche accidentale, o accesso non autorizzato ai dati.
- Il Comune deve assolvere all'obbligo di informativa sulle finalità perseguite con i sistemi di videosorveglianza e sui diritti riconosciuti agli interessati mediante l'affissione di cartelli-avvisi in prossimità delle telecamere o degli impianti di telecontrollo.

Grazie per l'attenzione

Il Codice della Privacy nella P.A.

Comune di Capoterra
4 e 5 ottobre 2009

LICENZA



Attribuzione - Non Commerciale - Condividi allo stesso modo 2.5

- Tu sei libero:
 - di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire o recitare l'opera
 - di creare opere derivate
 - Alle seguenti condizioni:
 - Attribuzione. Devi riconoscere il contributo dell'autore originario.
 - Non commerciale. Non puoi usare quest'opera per scopi commerciali.
 - Condividi allo stesso modo. Se alteri, trasformi o sviluppi quest'opera, puoi distribuire l'opera risultante solo per mezzo di una licenza identica a questa.
- In occasione di ogni atto di riutilizzazione o distribuzione, devi chiarire agli altri i termini della licenza di quest'opera.
- Se ottieni il permesso dal titolare del diritto d'autore, è possibile rinunciare ad ognuna di queste condizioni.
- Le tue utilizzazioni libere e gli altri diritti non sono in nessun modo limitati da quanto sopra