Comune di Castel Baronia
Provincia di Avellino

Manuale di Gestione Documentale
(art. 5 DPCM 3/12/2013)
Allegato 8 - Procedura Organizzativa
Amministratori di Sistema

Cod. **MANGEDOC** Rev. **1.0** Data: 20-07-2016

Sommario: Nel presente documento vengono descritte le modalità con cui l'Ente gestisce l'amministrazione dei sistemi, in rispondenza al Provvedimento del Garante per la protezione dei dati personali del 27-11-2008, pubblicato sulla G.U. n. 300 del 24-12-2008.

REVISIONI

Rev.	Data	Redattore/i	Descrizione
1.0	20-07-2016	Maria Pia Papa	Prima stesura

INDICE

1 SCOPO

Per meglio comprendere lo scopo di questa procedura, si riporta qui un estratto delle considerazioni preliminari del Garante per la protezione di dati personali che dà una perfetta definizione di “amministratore di sistema”.

<< Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

… omissis …

le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.>>

1.1 Applicabilità

Destinatari di questo documento sono gli amministratori di sistema nonché responsabili ed incaricati designati dall’Ente.

1.2 Obiettivo

L'obiettivo di questa procedura è quello di individuare alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito del Comune, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

L’Amministrazione Comunale intende prestare attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema, data la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni.

1.3 Oggetto

Amministrazione delle banche dati informatiche e dei sistemi su cui sono installate.

2 NORMATIVA DI RIFERIMENTO

Sulla G.U. n. 300 del 24 dicembre 2008 è stato pubblicato il provvedimento del Garante per la Protezione dei dati personali, emesso il 27-11-2008, riguardante:

"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008".

Con tale provvedimento il Garante per la protezione dei dati personali,

1. Ai sensi dell'art. 154, comma 1, lett. h) del Codice, nel segnalare a tutti i titolari di trattamenti di dati personali effettuati con strumenti elettronici la particolare criticità del ruolo degli amministratori di sistema, richiama l'attenzione dei medesimi titolari sull'esigenza di valutare con particolare attenzione l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema (system administrator), amministratore di base di dati (database administrator) o amministratore di rete (network administrator), laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali. Ciò, tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità sulla base delle quali si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato;

2. ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive l'adozione delle seguenti misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice ed effettuati con strumenti elettronici, anche in ambito giudiziario e di forze di polizia (artt. 46 e 53 del Codice), salvo per quelli effettuati in ambito pubblico e privato a fini amministrativo-contabili che pongono minori rischi per gli interessati e sono stati oggetto delle misure di semplificazione introdotte per legge (art. 29 d.l. 25 giugno 2008, n. 112, conv., con mod., con l. 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008):

a. Valutazione delle caratteristiche soggettive

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

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

b. Designazioni individuali

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

c. Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza oppure, nei casi in cui il titolare non è tenuto a redigerlo, annotati

comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante.

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

d. Servizi in outsourcing

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

e. Verifica delle attività

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

f. Registrazione degli accessi

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

3. dispone che le misure e gli accorgimenti di cui al punto 2 del presente dispositivo siano introdotti, per tutti i trattamenti già iniziati o che avranno inizio entro trenta giorni dalla data di pubblicazione nella Gazzetta Ufficiale del presente provvedimento, al più presto e comunque entro, e non oltre, il termine che è congruo stabilire in centoventi giorni dalla medesima data; per tutti gli altri trattamenti che avranno inizio dopo il predetto termine di trenta giorni dalla pubblicazione, gli accorgimenti e le misure dovranno essere introdotti anteriormente all'inizio del trattamento dei dati.

3 MISURE ADOTTATE DAL COMUNE

Nel Comune di Castel Baronia è operativo il Sistema Informativo Comunale (S.I.C.) basato sulle applicazioni software censite.

3.1 Funzioni richieste all'Amministratore di Sistema

All'amministratore di sistema è stata affidata la gestione tecnica del S.I.C. a servizio dell'Amministrazione Comunale e della cittadinanza, al fine di assicurare qualità ed efficienza dei servizi offerti dall'Ente, attraverso

- la tenuta in esercizio dei sistemi hardware e degli apparati attivi di trasmissione e ricezione dati;
- il monitoraggio e tuning dei sistemi, ovvero, il controllo continuo dei sistemi in esercizio, con una valutazione periodica delle performance, al fine di garantire un servizio efficiente degli applicativi software attivi ed una elevata disponibilità del servizio durante il normale orario di lavoro;
- il back-up e restore dei dati, cioè, le attività di salvataggio e ripristino dei dati relativi alle applicazioni software in esercizio.
- le attività sistemistiche riguardanti la sicurezza delle postazioni di lavoro, la rete, i server e le basi di dati, ai sensi del D. Lgs. 109/03.

Per raggiungere queste finalità il S.I.C. necessita di un presidio costante con attività sistemistiche, di amministrazione dei sistemi (macchine server, applicazioni software, banche dati) e della rete.

a) Gestione dei sistemi informatici

- Controllo costante del sistema informativo con attività sistemistiche e di amministrazione dei sistemi e della rete:
  - ***Tenuta in esercizio***

    Vengono svolte le attività per la tenuta in esercizio dei sistemi hardware e degli apparati attivi di trasmissione e ricezione dati. Per tali sistemi saranno gestite le attività di accensione e spegnimento e quelle di ripristino in caso di guasti o cadute.
  - ***Monitoring e Tuning***

    I sistemi in esercizio sono oggetto di controllo periodico con una valutazione delle performance, ciò al fine di garantire un servizio efficiente degli applicativi software attivi ed una elevata disponibilità del servizio durante il normale orario di lavoro.
  - ***BackUp e Restore dei dati***

    Sono garantite le attività per il salvataggio e ripristino dei dati relativi alle applicazioni software in esercizio. Il tutto in modalità conforme ai dettami emanati dal codice sul trattamento dei dati personali, di cui al D.Lgs. 196/03.
  - ***Assistenza sistemistica sulle postazioni di lavoro***

    Viene fornita assistenza sulle diverse postazioni di lavoro dei dipendenti degli Enti associati, tenendo sotto costante controllo anche tutti gli aspetti di sicurezza dei dati (autenticazione e autorizzazione, sistemi anti-virus e anti-intrusione, organizzazione file system e repository di dati sicuri)
  - ***Assistenza sistemistica sulle reti***

    Viene garantita l'assistenza sistemistica sulla rete locale.

    Vengono, in merito, gestiti i seguenti servizi:

a) il controllo della rete dati dal punto di vista della sicurezza e dell'anti-intrusione.

b) il controllo del traffico dati con la misurazione periodica delle performance al fine di garantire un servizio efficiente e con elevata disponibilità durante il normale l'orario di lavoro.

3.2 Misure e accorgimenti adottati

Per quanto riguarda le misure e gli accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, sono state poste in essere le seguenti azioni:

a. Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di Amministratore di Sistema è avvenuta previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

b. Designazioni individuali

La designazione quale Amministratore di Sistema è individuale e riporta l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, così come descritti nella prima parte di questo paragrafo.

c. Elenco degli Amministratori di Sistema

Gli estremi identificativi dell'Amministratore di Sistema, con l'elenco delle funzioni ad esso attribuite, sono riportati nel presente documento.

E' resa nota o conoscibile l'identità dell' Amministratore di Sistema nell'ambito dell'Amministrazione Comunale, tramite l'informativa resa agli interessati ai sensi dell'art. 13 del Codice nell'ambito del rapporto di lavoro che li lega al titolare, e tramite il disciplinare tecnico di cui al provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58).

d. Servizi in outsourcing

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare conserva direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema.

e. Verifica delle attività

L'operato dell'Amministratore di Sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

f. Registrazione degli accessi

Sono stati adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte dell'amministratore di sistema.