

REGIONE PUGLIA
ASL BA
AZIENDA SANITARIA LOCALE DELLA PROVINCIA DI BARI

DELIBERAZIONE DEL DIRETTORE GENERALE

Deliberazione n. 0600 del - 5 APR. 2011

OGGETTO: D.lgs n. 196/2003 e s.m.i - Individuazione degli Amministratori di Sistema - Adempimenti organizzativi alla luce del Provvedimento del Garante per la Protezione dei Dati Personali del 27/11/2008

L'anno 2011, il giorno cinque del mese di aprile in Bari, nella sede della A.S.L. al Lungomare Starita n. 6,

IL DIRETTORE GENERALE

- Visto il D.Lgs. 30/12/1992 n. 502 e successive integrazioni e modifiche;
- Vista la Legge Regionale 28/12/1994 n. 36;
- Vista la Legge Regionale 30/12/1994 n. 38
- Vista la Legge Regionale 03/08/2006 n. 25;
- Vista la Legge Regionale 28/12/2006 n. 39;
- Vista la Deliberazione della Giunta Regionale n. 1960 del 20.10.2009;
- Vista la Deliberazione della Giunta Regionale n. 2151 del 13.11.2009;

Sulla base di conforme istruttoria dell'Ufficio Privacy

HA ADOTTATO

Il seguente provvedimento

IL DIRETTORE AMMINISTRATIVO
Francesca LIPPOLIS

Visto, esprime parere _____

IL DIRETTORE SANITARIO
Rosa Porfido

Visto, esprime parere _____

IL DIRETTORE GENERALE
Nicola PANZINI

La presente deliberazione è trasmessa al Collegio Sindacale e viene pubblicata sul sito web aziendale nel rispetto di quanto disposto dalla L.R. n. 40/2007

IL RESPONSABILE DELLA SEGRETERIA

Si dichiara che il presente atto è copia conforme all'originale
Esso è composto da n. 5 fogli
Bari, - 5 APR 2011

Il Funzionario Coordinatore
della Segreteria Direzionale
A.S.L. BA
(Sig. Giuseppe Colella)

Premesso che:

- il 1° gennaio 2004 è entrato in vigore il D.Lgs 30.6.2003, n. 196 "Codice in materia di protezione dei dati personali", il quale prevede:
 - all'articolo 31 che "i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta";
 - agli articoli 34 e 35 che il Documento Programmatico sulla Sicurezza sia la misura cardine dell'intero impianto costruito dal legislatore al fine di assicurare un livello minimo di sicurezza nonché la fonte principale di tutte le misure minime tra loro strettamente connesse;

Accertato che:

- con deliberazione n. 455 del 16.03.2011 è stato approvato l'aggiornamento del Documento Programmatico sulla Sicurezza sulla base delle informazioni rilevate in seguito all'analisi ed allo studio dell'assetto organizzativo dei servizi e delle funzioni della medesima Azienda;

Considerato che:

- che il Provvedimento del Garante per la protezione dei dati personali del 27.11.2008 – "Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema":
 1. segnala a tutti i Titolari del trattamento di dati personali effettuati con strumenti elettronici, la particolare criticità del ruolo di Amministratore di Sistema, richiamando l'attenzione dei medesimi Titolari sulla necessità di adottare idonee misure tese a prevenire, ed eventualmente accertare, accessi non consentiti ai dati personali, richiamando inoltre l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di Amministratore di Sistema;
 2. stabilisce che l'attribuzione delle funzioni innanzi dette, deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato;

Considerato che:

- che all'interno dell'ASL Bari i sigg.ri dipendenti Massimo Scirucchio e Nicola Marino, personale a tempo indeterminato già impegnati nell'ambito dei Sistemi Informativi Aziendali, hanno dato prova di adeguata capacità e affidabilità tecnica, che dalla loro esperienza professionale emerge una accertata ed opportuna formazione professionale in relazione all'attribuzione della nomina di Amministratore di Sistema, confermata, questa loro preparazione, anche dal Dirigente Sistemi Informativi Aziendali, Ing. Maurizio Stasolla;

Ritenuto, pertanto:

- che sussistono le condizioni di legge e regolamentari per poter affidare ai dipendenti Massimo Scirucchio e Nicola Marino l'incarico di "Amministratore di sistema", come da allegata lettera di incarico, parte integrante del presente provvedimento, a firma del Direttore Generale su proposta del Dirigente Sistemi Informativi Aziendali, Ing. Maurizio Stasolla;

Dato atto che:

- dal presente provvedimento non derivano oneri per l'Azienda, se non quelli derivanti dalle prestazioni che normalmente il predetto personale svolge all'interno dell'U.O. Sistemi Informativi Aziendali;

Tanto premesso:

- si propone l'adozione del presente atto che autorizza i dipendenti Massimo Scirucchio e Nicola Marino a svolgere anche l'attività di "Amministratore di Sistema" per garantire quanto specificato e descritto nell'allegato documento di nomina che forma parte integrante del presente provvedimento;

Acquisiti i pareri del Direttore Amministrativo e del Direttore Sanitario

DELIBERA

-per le ragioni precisate in narrativa che qui si intendono integralmente riportate e confermate -

A) di prendere atto di quanto descritto in narrativa circa la necessità di nominare, in ottemperanza a quanto previsto dal Garante per la protezione dei dati personali, gli Amministratori di Sistema dell'ASL di Bari;

B) di prendere atto che all'interno dell'ASL di Bari, su proposta del Dirigente Sistemi Informativi Aziendali, Ing. Maurizio Stasolla, i dipendenti Massimo Scirucchio e Nicola Marino, già da tempo impegnati nell'ambito della U.O. Sistemi Informativi Aziendali, hanno dato prova di adeguata capacità e affidabilità tecnica in relazione all'attribuzione di nomina di Amministratori di Sistema della ASL di Bari;

C) di approvare e sottoscrivere la lettera di incarico proposta dal Dirigente Sistemi Informativi Aziendali, Ing. Maurizio Stasolla, con cui si affida l'attività di "Amministratore di Sistema", documento che si allega alla presente deliberazione per farne parte integrante;

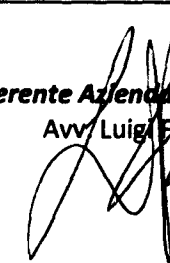
D) di determinare la durata minima del presente incarico in anni uno, e che la stessa nomina si riterrà tacitamente rinnovata salva diversa determinazione tra l'Azienda e i dipendenti interessati;

E) di dare mandato al Referente Aziendale della Privacy, Avv. Luigi Fruscio, di trasmettere la presente deliberazione al Dirigente Sistemi Informativi Aziendali, Ing. Maurizio Stasolla, e ai dipendenti Massimo Scirucchio e Nicola Marino ;

F) dare atto che dal presente provvedimento non derivano oneri per l'Azienda;

La presente deliberazione è trasmessa al Collegio Sindacale e viene pubblicata sul sito web aziendale nel rispetto di quanto disposto dalla L.R. n. 40/2007

Il Referente Aziendale della Privacy
Avv. Luigi Fruscio



NOMINA AMMINISTRATORE DI SISTEMA E ISTRUZIONI

(ai sensi del Codice in materia di protezione dei dati personali e del Provvedimento del Garante per la protezione dei dati personali del 27/11/2008)

PREMESSO in diritto

- che il Codice:
 - definisce Incaricati le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
 - stabilisce che le operazioni di trattamento possono essere effettuate solo da Incaricati, che operano sotto la diretta autorità del Titolare o del Responsabile, designate per iscritto, con individuazione puntuale dell'ambito del trattamento consentito;
- che il Garante per la protezione dei dati personali con Provvedimento n. 13 del 1° marzo 2007 ha rilevato che:
 - compete ai datori di lavoro, nel rispetto delle norme in tema di diritti e relazioni sindacali, assicurare la funzionalità e il corretto impiego di internet ed email da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa ed **adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;**
 - **nell'individuare regole di condotta degli Amministratori di sistema o figure analoghe deve essere svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni;**
- che il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, fra l'altro:
 - **segnala a tutti i Titolari la particolare criticità del ruolo degli Amministratori di sistema e la necessità di adottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali, in specie quelli realizzati con abuso della qualità di Amministratore di sistema;**
 - richiama l'attenzione sull'esigenza di valutare con particolare cura l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di Amministratore di sistema (laddove queste siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali), tenendo in considerazione l'opportunità o meno di tale attribuzione e le concrete modalità con cui si svolge l'incarico, unitamente alle qualità tecniche, professionali e di condotta del soggetto individuato, da vagliare anche in considerazione delle responsabilità, specie di ordine penale e civile;
 - prescrive al riguardo ai Titolari accorgimenti e misure ai sensi dell'art. 154, comma 1, lett. c) del Codice e fra l'altro che:
 - **l'attribuzione delle funzioni di Amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, che deve fornire idonea garanzia del pieno rispetto delle norme in materia di trattamento di dati, compreso il profilo relativo alla sicurezza;**
 - **la designazione quale Amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;**
 - **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 del Codice;**
 - **siano previste forme per consentire la conoscibilità dell'identità degli Amministratori di sistema, per registrarne gli accessi e per verificarne periodicamente l'operato;**
 - **che i dati personali devono essere trattati e conservati nel rispetto del Codice, delle altre norme e dei Provvedimenti del Garante per la protezione dei dati personali e delle misure di sicurezza, delle disposizioni, istruzioni, procedure, policy del Titolare e del Responsabile;**
 - **che per qualsiasi necessità o per la risoluzione di qualsiasi problematica inerente al trattamento gli Incaricati e gli Amministratori di sistema dovranno rivolgersi al Responsabile e/o Titolare.**

PREMESSO in fatto

- che l'Azienda Sanitaria ASL Ba, con sede legale in Via Lungomare Starita,6 a Bari , C.F. 06534340721 é Titolare del trattamento dei dati personali effettuati anche mediante strumenti elettronici;
- che per necessità organizzative è stata adottata una politica di distribuzione compiti e responsabilità ICT per ambiti di operatività, come di seguito specificato :
 - A. Manutenzione ed Assistenza su PDL
 - B. Manutenzione ed Assistenza su Server di rete
 - C. Sicurezza e monitoraggio Rete e Pc
- che i Sigg. SCIRUICCHIO MASSIMO e MARINO NICOLA si dichiarano e sono effettivamente soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati, ivi compreso il profilo relativo alla sicurezza;
- che i Sigg. SCIRUICCHIO MASSIMO e MARINO NICOLA svolgono attività che, ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, è definibile di Amministratore di sistema;

Tutto ciò premesso, il Titolare

dopo essersi attenuto a criteri di valutazione equipollenti a quelli richiesti per la designazione dei Responsabili ai sensi dell'art. 29 del Codice, avendo valutata l'esperienza, la capacità e l'affidabilità dei designati, tenuto anche conto del curriculum e del suo contenuto (inclusi, attività svolte, titoli di studio, certificazioni professionali, esperienze professionali, corsi di formazione, ecc.), considerata la natura delle attività da essi attualmente svolte, considerato che con la sottoscrizione della presente gli stessi si impegnano formalmente a fornire, ed appaiono idonei a fornire, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati ivi compreso il profilo relativo alla sicurezza

Designa

- i predetti Sigg. SCIRUICCHIO MASSIMO e MARINO NICOLA, Amministratori di sistema (ambiti A, B e C come su specificati), ed indica analiticamente gli ambiti di operatività consentiti agli stessi in base al profilo di autorizzazione assegnato e precisamente :
 - A. Manutenzione ed Assistenza su PDL: SCIRUICCHIO MASSIMO e MARINO NICOLA
 - B. Manutenzione ed Assistenza su Server di rete: SCIRUICCHIO MASSIMO e MARINO NICOLA
 - C. Sicurezza e monitoraggio Rete e Pc: SCIRUICCHIO MASSIMO e MARINO NICOLA

Con la sottoscrizione del presente atto il i Sigg. SCIRUICCHIO MASSIMO e MARINO NICOLA accettano le designazioni suddette, confermano la propria esperienza e capacità nella materia nonché la diretta ed approfondita conoscenza degli obblighi previsti dal Codice e/o altre norme applicabili, dai Provvedimenti del Garante, e dalla normativa e procedure aziendali e dalla presente. Si impegnano a procedere al trattamento dei dati personali attenendosi quindi a quanto stabilito dalla normativa e Provvedimenti in materia ed in conformità alle istruzioni impartitegli dal Titolare e dal Responsabile, nonché alle disposizioni, policy, procedure e regolamenti aziendali

informa i designati che

- gli estremi identificativi delle persone fisiche Amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, saranno riportati nel documento programmatico sulla sicurezza;
- qualora l'attività riguardi, o dovesse in futuro riguardare, anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, il Titolare renderà nota o conoscibile l'identità del designato nell'ambito della propria organizzazione, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici, conformemente e con le modalità previste dal Garante per la protezione dei dati personali e dalle norme;
- sono adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di sistema e quindi dei designati;
- le registrazioni (access log) comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate ed hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. In ogni caso è tassativamente vietato intervenire in

alcun modo su di esse (ad es. cancellando- le, modificandole, alterandole, ecc. o compiendo qualsiasi altra attività sulle stesse). Le registrazioni sono conservate per almeno sei mesi;

- l'operato dei designati sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti e precisamente

fornisce le seguenti istruzioni ai designati

precisando che rimangono ferme e confermate le precedenti istruzioni, regolamenti aziendali, procedure e policy, in quanto non espressamente derogate dalla presente e/o non incompatibili con la stessa.

Particolare cura i designati devono prestare al rispetto delle misure di sicurezza dei dati, minime ed ulteriori, adottate per il trattamento dei dati con strumenti elettronici o senza. I designati devono quindi applicare le misure minime ed ulteriori e compiere tutte le attività di competenza necessarie al fine di garantire il corretto funzionamento di esse anche con riferimento agli strumenti elettronici affidati o con riferimento ai quali svolgono attività di manutenzione, assistenza, sviluppo, ecc..

In ogni caso i designati potranno trattare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati e/o comunque i soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento e per svolgere le attività attribuite e le mansioni di competenza.

I designati devono sempre tenere conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia (artt. 1 e 2 del Codice).

Nelle attività da svolgere con riferimento agli strumenti informatici si devono inoltre e sempre applicare:

- il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice);
- il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice);
- il principio in forza del quale i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice), osservando il principio di pertinenza e non eccedenza, trattando i dati «nella misura meno invasiva possibile»; eventuali attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere mirate sull'area di rischio, tenendo conto della normativa in materia.

Vanno inoltre sempre applicate le norme ed i Provvedimenti del Garante, incluso esemplificativamente quello n. 13 del 1 marzo 2007 al cui contenuto, così come quello del 27 novembre 2008, si rinvia.

I trattamenti dei designati devono essere ispirati ad un canone di liceità, trasparenza e correttezza.

Nel caso di interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti ed i soggetti preposti debbono svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza.

È tassativamente vietato qualsiasi trattamento effettuato con sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l'attività di lavoratori.

In applicazione del menzionato principio di necessità il Titolare promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a minimizzare l'uso di dati riferibili ai lavoratori.

Per quanto attiene agli eventuali controlli sull'uso degli strumenti elettronici deve essere evitata ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. Infatti, come è noto, gli eventuali controlli sono leciti solo se sono rispettati i principi di pertinenza e non eccedenza. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Titolare può adottare eventuali misure che consentano la verifica di comportamenti anomali, preferendo controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

La conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata solo da particolari esigenze tecniche o di sicurezza, o da una finalità specifica e comprovata e limitata al tempo necessario- e predeterminato - a raggiungerla (v. art. 11, comma 1, lett. e), del Codice). Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali n. 1 e 5 del 2008 adottate dal Garante ed eventualmente dell'autorizzazione n. 7 del 2008 per i dati giudiziari) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Resta fermo l'obbligo dei designati di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità legalmente previste, senza realizzare attività di controllo a distanza.

All'atto della cessazione del rapporto con il Titolare i designati dovranno in ogni caso restituire tutti i dati personali trattati con espresso e formale divieto di conservarli, duplicarli, ecc.

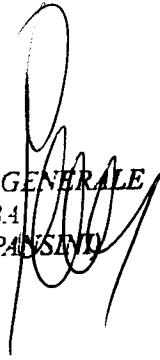
La designazione di Amministratore di sistema (in qualità di incaricato al trattamento) si dovrà considerare comunque automaticamente revocata alla cessazione del rapporto di lavoro sopra indicato.

La presente individuazione dell'ambito del trattamento dei dati, che deriva dall'applicazione di norme imperative, non comporta alcuna modifica retributiva e/o contrattuale e/o mansionistica al rapporto di lavoro degli addetti/Incaricati.

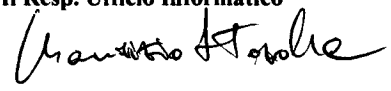
Bari,

**Il Titolare
D.G.**

*IL DIRETTORE GENERALE
ASL B4
(Dr. Nicola PASSINI)*



Il Resp. Ufficio Informatico



Gli Amministratori di Sistema (ambiti A, B e C come su specificato)

MASSIMO SCIRUICCHIO



NICOLA MARINO

