COMUNE DI USSASSAI

PROVINCIA DELL'OGLIASTRA

Indirizzo: Via Nazionale, 120 – C.A.P. 08040 – Ussassai

E-Mail protocollo@pec.comune.ussassai.og.it Sito web: http://www.comune.ussassai.og.it

☎0782/55710 🖷 0782/55890

C.F. e P.IVA 00160240917

Registro Settore N° 2 del 17/01/2011

AREA AMMINISTRATIVA SOCIALE TRIBUTI

DETERMINAZIONE
DEL RESPONSABILE DEL SERVIZIO AMMINISTRATIVO

N.R.G.	DATA	OGGETTO:
2	17/01/2011	D.LGS.N.196/2003 - PROVVEDIMENTO DELL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 27.11.2008 G.U. N. 300 DEL 24/12/2008 COSÌ COME MODIFICATO DAL PROVVEDIMENTO A CARATTERE GENERALE DELL'AUTORITÀ GARANTE DEL 25/06/2009 G.U. N. 149 DEL 30/06/2009 - DESIGNAZIONE DEL NUOVO AMMINISTRATORE DEL SISTEMA INFORMATICO DELL'ENTE IN SOSTITUZIONE DEL DOTT. L. C.

Il Responsabile del Servizio

PREMESSO CHE:

- il D. Lgs. 196/03, recante "Codice in materia di protezione dei dati personali", impone alle Pubbliche Amministrazioni titolari del trattamento dei dati personali, l'adozione di "misure minime di sicurezza", volte ad evitare - sulla base di idonee misure organizzative, logistiche e procedurali - un incremento dei rischi connessi al trattamento con strumenti elettronici dei dati personali, sensibili e giudiziari, detenuti per finalità connesse al perseguimento degli scopi istituzionali;
- l'Amministrazione Comunale possiede un sistema informatico e pertanto ai sensi del citato D. Lgs. 196/03 occorre nominare un Amministratore di sistema che si occupi della predisposizione e gestione delle misure di sicurezza adottate a tutela del sistema informatico stesso, della protezione dei dati informatici, delle proposte di nuove misure di protezione dei dati in conformità al progresso tecnologico, della gestione dei codici identificativi personali prevedendo la disattivazione in ipotesi di mancato utilizzo dei medesimi per un periodo temporale superiore ai sei mesi, della protezione con adeguati programmi antivirus degli elaboratori e del loro aggiornamento secondo la periodicità prevista dalla normativa vigente;
- il Garante per la Protezione dei Dati Personali, con Provvedimento generale del 27/11/2008 (G.U. n. 300 del 24/12/08) "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema", ha prescritto specifiche misure ai titolari dei trattamenti di dati personali soggetti all'ambito applicativo del Codice sulla Privacy (D.Lgs. n. 196/2003) ed effettuati con strumenti elettronici;
- secondo quanto espressamente previsto ai Punti 4.2 e 4.3 del richiamato Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27.11.2008 così come modificato dal Provvedimento a carattere Generale dell'Autorità Garante del 25/06/2009, 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 e che gli estremi identificativi delle persone fisiche amministratori

di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante;

DATO ATTO

- Che con determinazione n. 60 del 04.11.2010 è stato affidato alla S.I.P.A.L. srl di Cagliari il Servizio di Amministratore del Sistema Informatico dell'Ente e di affiancamento formativo al proprio personale dipendente per il periodo un anno (0101.2011-31.12.2011);
- Che la S.I.P.A.L. srl ha individuato la figura dell'Amministratore del sistema informatico dell'Ente nella persona del Tecnico Informatico Dott. Luigi Cadau, nato a Nuoro il 16/04/1974, dipendente della citata Società;
- Che la S.I.P.A.L. srl di Cagliari ha provveduto a comunicare con nota del 11.01.20 prot. n. 0040/2011 che il Dott. Luigi Cadau ha presentato le proprie dimissioni volontarie alla Società in data 30/12/2010 con decorrenza dal medesimo giorno in quanto vincitore di pubblico concorso;
- Che la S.I.P.A.L. srl con la medesima nota ha provveduto a comunicare all'Ente i nominativi dei tecnici informatici dipendenti strutturati della stessa Società, che dovranno essere designati dall'Ente come Amministratori di sistema in sostituzione del Dott. Luigi Cadau, come di seguito generalizzati:
  - **Dott. Gianmario Lai, nato a Sassari il 14/11/1981, residente in Uri (SS) nel Largo Cavour, al civico 1,**
  - **Dott.ssa Ing. Eleonora Mutzu Martis, nata a Sassari il 25/10/1980, residente in Sassari nella Via Luna e Sole al civico 52/21**;
- Che la S.I.P.A.L. srl ha preventivamente verificato la sussistenza in capo ai citati tecnici informatici dei requisiti di esperienza, capacità ed affidabilità prescritti al Punto 4.1 del Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27.11.2008 così come modificato dal Provvedimento a carattere Generale dell'Autorità Garante del 25/06/2009;

DETERMINA

Per quanto esposto in premessa,

DI DESIGNARE in sostituzione del Dott. Luigi Cadau, il **Dott**. **Gianmario Lai**, nato a Sassari il 14/11/1981, residente in Uri (SS) nel Largo Cavour, 1 e la **Dott.ssa Ing. Eleonora Mutzu Martis**, nata a Sassari il 25/10/1980, residente in Sassari nella Via Luna e Sole n. 52/21, dipendenti a tempo pieno ed indeterminato della S.I.P.A.L. srl di Cagliari, quali Amministratore del sistema informatico Comunale con i compiti e le funzioni di seguito indicati conformemente a quanto previsto dall'art. 34 D. Lgs. 196/03 e dalla Regola 19 dell'Allegato B al Codice in materia di protezione dei dati personali.

In particolare, gli Amministratori di sistema, sono personalmente incaricati:

- Dell'affiancamento all'Ente nella definizione delle politiche informatiche e nella redazione del relativo piano di sviluppo triennale in conformità ai principi dell'Amministrazione Digitale ed alle linee guida emanate dal CNIPA;
- Dell'esecuzione degli accessi tecnici presso l'Ente, al fine di garantire il corretto funzionamento, l'evoluzione e l'implementazione del sistema informativo dell'Ente;
- Dell'assunzione della funzione di interfaccia tecnica tra l'Ente ed i fornitori di hardware e software al fine di garantire l'individuazione, condivisa, delle migliori soluzioni tecnicamente disponibili secondo il principio della efficacia e dell'economicità della spesa;

- Dell’esecuzione di giornate di formazione, organizzate in sedi baricentriche e presso le quali convergeranno gli Enti del territorio, dedicate ai lavoratori di ciascuna Amministrazione ed aventi ad oggetto le materie ovvero le attività per le quali si sia rilevata una situazione di criticità emersa durante la gestione del sistema informativo;
- Dell’affiancamento formativo reso in favore del Responsabile Informatico interno, ai fini dell’acquisizione delle competenze per l’assunzione dell’incarico di Amministratore di Sistema Interno;
- Della gestione dei sistemi di autenticazione informatica con riferimento al personale costituente la dotazione organica dell’Ente, ai lavoratori a tempo determinato, ai collaboratori, agli addetti alla manutenzione hardware e software con obbligo di sostituzione autonoma della componente riservata della credenziale di autenticazione con periodicità semestrale in caso di trattamento di dati personali e trimestrali nell’ipotesi di trattamento di dati sensibili e giudiziari;
- Dell’attribuzione di credenziali di autenticazione strutturate per mantenere caratteristiche di robustezza, inviolabilità nel rispetto della segretezza della componente riservata della credenziale di autenticazione ai sensi delle vigenti normative con correlata attività di costante informazione rivolta ai lavoratori in ordine alle metodiche di gestione delle stesse credenziali al fine di garantire la salvaguardia dei requisiti di disponibilità, integrità e riservatezza dei dati;
- Della gestione dei profili di autorizzazione in conformità alla organizzazione degli uffici e dei servizi e delle funzioni eventualmente attribuite all’esterno;
- Della definizione e messa a regime delle procedure per l’adozione di sistemi di protezione contro il rischio di intrusione e dell’azione di programmi di cui all’art. 615-quiquies del codice penale mediante l’attivazione di idonei strumenti elettronici con cadenza almeno semestrale;
- Della definizione e messa a regime delle procedure di adozione di aggiornamenti periodici di programmi per elaboratore volti a prevenirne le vulnerabilità ed a correggerne i difetti con cadenza almeno annuale per il trattamento di dati personali e semestrale in caso di trattamento di dati sensibili e giudiziari;
- Della definizione e messa a regime delle procedure per l’esecuzione di copie di sicurezza che garantiscano l’Ente contro il rischio di perdita di dati e consentano, in caso di evento dannoso, l’avvio del Piano di Continuità Operativa;
- Della definizione e messa a regime delle procedure contro l’accesso abusivo a dati sensibili e giudiziari di cui all’art. 615-ter del codice penale mediante l’utilizzo di idonei sistemi elettronici;
- Della definizione e messa a regime delle procedure per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti;
- Della definizione e messa a regime delle procedure preordinate a garantire che i supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati siano distrutti o resi inutilizzabili, ovvero possano essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non siano intelligibili e tecnicamente in alcun modo ricostruibili;
- Della definizione e messa a regime delle procedure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

DI DARE ATTO che l’Ente provvederà ad adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) da parte dell’Amministratore ai sistemi di elaborazione ed agli archivi elettronici dell’Ente. Le registrazioni (*access log*) avranno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per

cui sono richieste. Le citate registrazioni comprenderanno i riferimenti temporali e la descrizione dell'evento che le ha generate e saranno conservate per un congruo periodo di tempo, non inferiore a sei mesi. La raccolta dei *log* servirà per verificare eventuali anomalie nella frequenza degli accessi e nelle loro modalità (orari, durata, sistemi cui si è fatto accesso). L'analisi dei *log* sarà ricompresa tra i criteri di valutazione dell'operato dell' Amministratore di sistema.
In particolare, si provvederà alla registrazione di tutti gli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte dell'Amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi *software*.
Gli *event records* generati dai sistemi di autenticazione conterranno i riferimenti allo "username" utilizzato, alla data e all'ora dell'evento (*timestamp*) ed una descrizione dell'evento (sistema di elaborazione o *software* utilizzato, se si tratti di un evento di *log-in*, di *log-out*, o di una condizione di errore, quale linea di comunicazione o dispositivo terminale sia stato utilizzato).
Gli eventi censiti nel sistema di *log*, comprenderà tutti gli eventi di accesso interattivo che interessino l'Amministratore di sistema su tutti i sistemi di elaborazione con cui vengono trattati, anche indirettamente, dati personali.

CERTIFICATO DI PUBBLICAZIONE

La presente determinazione viene pubblicata mediante affissione all'Albo Pretorio *on–line* del Comune per 15 giorni consecutivi a decorrere dal 17/01/2011

Ussassai, 17/01/2011

L'addetto alle Pubblicazioni
Dott.ssa Lisa Mura