AREUS
Azienda Regionale
Emergenza Urgenza
Sardegna

REGIONE AUTONOMA DELLA SARDEGNA

Egr.

Sig./Sig.ra Dott./ Dott.ssa _____,

Indirizzo _____

Matricola n. _____,

C.F.: _____,

in servizio presso l'Area _____

OGGETTO: Nomina ad Amministratore di Sistema nell'ambito del trattamento e della protezione dei dati, ai sensi del Regolamento UE 2016/679

Il Titolare del trattamento

VISTI:

- il Regolamento EU 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali – nel seguito, "**General Data Protection Regulation**" o "**GDPR**";

- il Decreto Legislativo 30 giugno 2003 n. 196 (Codice Privacy) come modificato dal Decreto legislativo 10 agosto 2018 n. 101 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 2016/679);

- il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, pubblicato nella G. U. n. 300 del 24 dicembre 2008, e successive modificazioni intervenute con il Provvedimento del 25 giugno 2009, pubblicato nella G.U. n. 149 del 30 giugno 2009;

- la Delibera N. Prot. ….del …… di approvazione del regolamento sull'utilizzo della strumentazione informatica interna e della rete Internet, del Direttore Generale di AREUS – Azienda Regionale Emergenza Urgenza Sardegna (di seguito anche "**AREUS**" o "**Ente**");

- la Delibera N. Prot. ….del …… di nomina degli Amministratori di Sistema;

* * *

In considerazione delle Sue comprovate competenze ed esperienze, nonché del grado di affidabilità richiesto per l'adempimento dei compiti connessi alla presente nomina, con la presente La nominiamo "**Amministratore di sistema**" ai sensi del Regolamento UE 2016/679 e del provvedimento generale del Garante per la Protezione dei Dati Personali in data 27 novembre 2008 e pubblicato sulla G.U. n. 300 del 24.12.2008 e successive modifiche.

COMPITI E RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA

All'Amministratore di Sistema vengono attribuiti i seguenti compiti:

- Installare, gestire e monitorare le risorse hardware e software del sistema informativo e del sistema di videosorveglianza dell'Ente, anche con l'ausilio di personale esterno appositamente designato;
- Effettuare interventi di manutenzione e aggiornamento dell'hardware e del software del sistema informativo, sia lato server che client, anche con l'ausilio di personale esterno appositamente designato;
- assicurare la progettazione e/o la messa in funzione delle soluzioni tecniche per garantire e gestire le misure di sicurezza adeguate richieste dal Regolamento UE 2016/679;
- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
- di autorizzare gli accessi dei singoli soggetti autorizzati ex art. 2-quaterdecies del D. Lgs. n. 196/2003, limitandone la possibilità di operare sulla base del proprio mansionario secondo le indicazioni che verranno trasmesse dal Titolare del trattamento;
- avere cura della custodia delle parole chiave per l'accesso al sistema informativo e gestire le password di root o di amministratore di sistema;
- individuare per iscritto il/i soggetto/i autorizzato/i della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla sua/loro attività;
- individuare per iscritto gli altri soggetti, diversi dall'/dagli autorizzato/i della custodia delle parole chiave, che possono avere accesso a informazioni che concernono le medesime;
- fare in modo che sia prevista la disattivazione dei "codici identificati personali" (User-ID), in caso di perdita della qualità che consentiva all'utente o autorizzato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei "codici identificativi personali" (User-ID) per oltre 6 mesi;
- assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery) anche automatici, nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS ecc.);
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
- predisporre un piano di controlli periodici, da eseguire con cadenza almeno semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate, nonché aggiornare con la medesima cadenza idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contrazione di virus informatici (antivirus, firewall ecc.);
- classificare analiticamente le banche dati e impostare/organizzare un sistema complessivo di trattamento dei dati personali comuni e particolari, predisponendo e curando ogni relativa fase applicativa nel rispetto della normativa vigente in materia di protezione dei dati personali;
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware, nonché la verifica di eventuali tentativi di accessi non autorizzati al sistema provenienti da soggetti terzi, quali accesso abusivo al sistema informatico o telematico, frode, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici;
- aggiornare periodicamente, con frequenza almeno annuale (o semestrale se si trattano dati particolari), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;

- adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici (anche effettuati 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 di verifica per cui sono richieste. Tali registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate ed essere conservate per un congruo periodo, non inferiore a sei mesi;
- dare tempestiva comunicazione al Titolare del trattamento dei dati personali qualora vengano rilevati rischi relativamente alle misure di sicurezza predisposte per la protezione dei dati trattati o una violazione di dati personali (Data Breach);
- descrivere dettagliatamente gli interventi che verranno eseguiti sui sistemi informatici mediante la compilazione di rapporti di intervento o di altri strumenti analoghi, dai quali si desuma: data dell'intervento, durata, tecnici che lo hanno effettuato, operazioni svolte, strumenti coinvolti (server, router, firewall, PC) o ogni altro dettaglio utile alla comprensione dell'intervento svolto;
- provvedere periodicamente a verificare l'opportunità di eventuali adeguamenti delle piattaforme hardware e software che si rivelino necessari a seguito del mutato quadro di conoscenze tecniche e informatiche;
- collaborare con il Titolare nel caso pervengano richieste di accesso ai dati personali da parte di terzi interessati o da parte delle Autorità (ad es. Organi di Polizia ecc.), per la cui evasione sia necessario l'intervento dell'Amministratore di Sistema, in tal caso, quest'ultimo si impegna a prestare tutta la collaborazione necessaria a dare riscontro alle richieste nei termini di legge;
- collaborare alla predisposizione o all'aggiornamento delle procedure interno riguardanti il trattamento dei dati personali e la sicurezza delle informazioni, per assicurare il pieno rispetto del GDPR in materia di trattamento dei dati personali;
- controllare l'accesso ai locali della sala macchine (eventuali tecnici esterni devono essere identificati ed autorizzati all'accesso, e devono operare sotto stretta sorveglianza di un Amministratore di sistema interno);
- disporre il blocco dei dati qualora sia necessaria una sospensione temporanea delle operazioni di trattamento, dando tempestiva comunicazione al Titolare del trattamento e/o ai suoi preposti;
- qualora si renda necessario per comprovati motivi di sicurezza dei sistemi, accedere a profili di trattamento dei singoli utenti.

All'Amministratore di Sistema è consentito operare, anche per mezzo di collegamenti dall'esterno purché effettuati con modalità tali da non compromettere la sicurezza complessiva del sistema, sui sistemi e sugli archivi e sui documenti in essi contenuti anche in presenza di dati personali particolari limitando i trattamenti e le operazioni a quelli necessari ai compiti precedentemente indicati.

L'Amministratore di Sistema testé designato:

- dichiara di essere a conoscenza di quanto stabilito dal Regolamento UE 2016/679 e della normativa relativa alla sicurezza e protezione dei dati vigente (ivi compresi i provvedimenti del Garante) e si impegna nell'adottare tutte le misure necessarie all'attuazione delle norme;
- dichiara di possedere l'esperienza, le qualità tecniche, professionali e di condotta, ovvero le competenze minime necessarie allo svolgimento del suddetto incarico, e pertanto lo si autorizza a svolgere i compiti assegnati secondo quanto previsto in dettaglio nell'Allegato A "**Ambito di competenza specifica per le attività di Amministratore di Sistema**", facente parte integrante del presente atto di nomina;

- si impegna nel mettersi a completa disposizione del Titolare per le attività di verifica, con cadenza almeno annuale, previste dalla normativa, al fine di controllare la rispondenza delle misure organizzative, tecniche e di sicurezza rispetto al trattamento dei dati.

Le modalità operative e le procedure di dettaglio per lo svolgimento delle mansioni sono rimandate a specifiche procedure operative o manuali interni di gestione.

Luogo e data: _____

Sottoscrive per accettazione e presa visione

L'Amministratore di Sistema *Il Titolare del Trattamento*

_____ _____

ALLEGATO A

Ambito di competenza specifica per le attività di Amministratore di Sistema

L'Amministratore di Sistema è abilitato ad operare sui seguenti sistemi:

- Server di rete del dominio aziendale (Active directory), sistemi di autenticazione degli utenti e profilazione, sistemi di autorizzazione;
- Postazioni utente del dominio aziendale e relative periferiche e accessori;
- Server e storage in utilizzo presso le sedi aziendali;
- Sistemi DBMS (Data Base Management System), Dataware House, di controllo accessi (Firewall, router, Intrusion Detection System, ecc…), di gestione (switch e apparati attivi di rete ecc…);
- Sistemi antivirus, antimalware, firewall ecc.
- Sistemi applicativi aziendali (Sistema AMC Amministrativo-contabile, Protocollo Informatico, Atti delibere e gestione documentale, Gestione del personale e delle timbrature ecc…);
- Sistemi di posta elettronica, anche certificata, sito Internet/Intranet, anche in Cloud (CMS: Content Management System);
- Sistemi telefonici e di telecomunicazione (Telefoni, server, centralino, apparati di networking ecc.);
- Sistemi di videosorveglianza e controllo accessi (Telecamere, server, orologi timbratori, lettori di badge ecc…);
- Ogni altro apparato in gestione dell'Area dei Sistemi Informativi e reti tecnologiche, quali, a titolo non esaustivo: tablet, cellulari, terminali fissi e mobili, periferiche, radiotrasmittenti, antenne e parabole di trasmissione ecc.
- <Indicare eventuali altri sistemi e software su cui l'AdS è autorizzato a operare>
-
-
-

In particolare, oltre ai compiti indicati nell'atto di nomina, egli avrà le seguenti mansioni, individuate dalla Direzione Aziendale e dal Responsabile dell'Area dei Sistemi informativi e reti tecnologiche:

<Indicare eventuali mansioni specifiche del singolo Amministratore di Sistema>

-
-
-