AREUS
Azienda Regionale
Emergenza Urgenza
Sardegna

REGIONE AUTONOMA DELLA SARDEGNA

Egr.

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

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. 43 del 3 marzo 2022 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. ** del ********** del Direttore Generale di AREUS con la quale si modifica dell'allegato al regolamento sull'utilizzo della strumentazione informatica interna e della rete internet.;

* * *

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;
- adottare il principio del 'privilegio minimo', operando esclusivamente sugli ambiti di competenza definiti nella presente nomina e nei relativi allegati. L'accesso ai sistemi avverrà solo per il tempo strettamente necessario all'adempimento delle mansioni assegnate. Qualsiasi accesso o intervento su dati personali, database o sistemi critici dovrà essere preventivamente autorizzato dal Titolare del trattamento, salvo emergenze documentate;
- 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;
- custodire in modo sicuro le credenziali di accesso ai sistemi informativi. È vietata la condivisione delle password di root o di amministratore con soggetti non autorizzati. L'Amministratore di Sistema è tenuto a utilizzare strumenti sicuri di gestione delle credenziali (es. sistemi di password vaulting) e a garantire la rotazione periodica delle stesse con frequenza almeno semestrale o secondo le diverse indicazioni scritte o policy del Titolare del trattamento. Qualsiasi tentativo di accesso non autorizzato dovrà essere immediatamente segnalato al Titolare del trattamento per gli adempimenti di competenza;
- 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. L'accesso ai log sarà consentito esclusivamente al Titolare del trattamento e/o al Responsabile della protezione dei dati (DPO), previa autorizzazione specifica, e in conformità alle disposizioni normative vigenti. Qualsiasi accesso ai log da parte dell'Amministratore di Sistema dovrà essere tracciato;
- segnalare immediatamente al Titolare del trattamento qualsiasi evento che possa costituire una violazione delle misure di sicurezza adottate o un potenziale data breach rilevante ai sensi della normativa in materia di protezione dei dati, compresi accessi non autorizzati, perdite di dati o malfunzionamenti critici dei sistemi. La segnalazione deve avvenire senza ritardo e comunque entro 24 ore dalla scoperta dell'evento, al fine di consentire l'attivazione tempestiva delle procedure di gestione dell'incidente e di eventuale notifica alle Autorità competenti;
- 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;
- 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;
- mantenere la massima riservatezza sui dati e sulle informazioni trattate nell'esercizio delle proprie funzioni. È vietato l'uso, la divulgazione o l'accesso ai dati per finalità diverse da quelle previste nella presente nomina. Qualsiasi violazione degli obblighi di riservatezza sarà considerata grave inadempienza e potrà comportare la revoca dell'incarico, oltre alle eventuali conseguenze di natura disciplinare, civile e penale;
- collaborare fattivamente nell'attuazione, ove necessario, degli adempimenti necessari a garantire la conformità del Titolare alla Direttiva UE n. 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022 nota anche come "Direttiva NIS2", nonché alla normativa nazionale di recepimento ed alle disposizioni dell'Autorità per la Cybersicurezza Nazionale o altra autorità competente in materia.

Accesso da remoto e dati personali particolari

All'Amministratore di Sistema è consentito operare sui sistemi e sugli archivi e sui documenti in essi contenuti per mezzo di collegamenti dall'esterno purché effettuati con modalità tali da non compromettere la sicurezza complessiva del sistema (es. VPN con autenticazione a due fattori). In presenza di dati personali particolari limiterà i trattamenti e le operazioni a quelli necessari allo svolgimento dei compiti precedentemente indicati. Qualsiasi attività svolta da remoto dovrà rispettare le medesime misure di sicurezza previste per gli accessi locali. È vietato l'uso di strumenti o software non autorizzati dal Titolare del trattamento per l'accesso ai sistemi aziendali.

* * *

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 relative 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 nei sistemi informatici del Titolare dettagliati nell'Allegato A "**Ambito di competenza specifica per le attività di Amministratore di Sistema**", facente parte integrante del presente atto di nomina nonché nei diversi sistemi/banche dati/applicativi sui quali sia stato specificamente autorizzato ad operare da parte del Titolare o suo delegato;
- si impegna nel mettersi a completa disposizione del Titolare o di un soggetto dallo stesso delegato 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, fornendo la documentazione necessaria e rendendosi disponibile per eventuali chiarimenti. A tal fine dichiara di aver letto e ben compreso la sottoestesa informativa sul trattamento dei dati di log da parte del Titolare.

Per quanto non previsto nel presente atto di nomina e per le modalità operative di dettaglio per lo svolgimento delle mansioni si rimanda a specifiche procedure di dettaglio o manuali interni di gestione, che l'Amministratore si impegna ad osservare scrupolosamente.

Luogo e data: _____

Sottoscrive per accettazione e presa visione

L'Amministratore di Sistema

Il Titolare del Trattamento

_____

AREUS
Azienda Regionale
Emergenza Urgenza
Sardegna

REGIONE AUTONOMA DELLA SARDEGNA

ALLEGATO A

Sistema	Descrizione sistema	Accesso amministrativo	Accesso amministrativo limitato	Nessun accesso amministrativo
ILO-ESXi01 e ILO-ESXi02	Server fisici ambiente virtualizzato			
vCenter	Gestore infrastruttura virtuale			
AVCP	File server / cartelle condivise e portale intranet (CMS: Content management System)			
SNU-DC01 e SNU-DC02	Server di dominio (Active Directory, Log accessi al dominio, DHCP, DNS)			
SNU-FS01	File Server / Backup cartelle “documenti”			
SNU-WSUS	Gestione pubblicazione aggiornamenti			
ME4024A	SAN (storage di rete)			
BitDefender	Servizio centralizzazione avvisi antivirus e hw inventory			
DBMS	- Specificare quali -			
Datawarehouse	- Specificare quali -			
PDL	Postazioni utente del dominio aziendale e relative periferiche e accessori			
Firewall	Filtraggio traffico internet con mantenimento log			
Switch	Apparati attivi infrastruttura di rete			
Sistemi Regionali	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			
Sistemi telefonici e di telecomunicazione	Telefoni, server, centralino, apparati di networking ecc.			
Sistemi di videosorveglianza	Telecamere, NVR, XVR			
Controllo accessi	orologi timbratori, lettori di badge			
Altro	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.			

AREUS
Azienda Regionale
Emergenza Urgenza
Sardegna

REGIONE AUTONOMA DELLA SARDEGNA

INFORMATIVA PRIVACY PER IL TRATTAMENTO DEI DATI DI LOG DELL'AMMINISTRATORE DI SISTEMA

Ai sensi dell'art. 13 del Regolamento UE 2016/679 (GDPR)

---

1. Titolare del Trattamento

Il Titolare del trattamento dei dati è l'Azienda Regionale Emergenza Urgenza Sardegna (AREUS) con sede in Nuoro, via Luigi Oggiano, contattabile ai seguenti riferimenti:

- Email: **[Email del Titolare]**
- PEC: **[PEC del Titolare]**

2. Responsabile della Protezione dei Dati (DPO)

Il Titolare ha designato un Responsabile della Protezione dei Dati (DPO), contattabile all'indirizzo email **dpo@areus.sardegna.it** per qualsiasi informazione relativa alla protezione dei dati personali.

3. Finalità del Trattamento e Base Giuridica

I dati di log dell'Amministratore di Sistema saranno trattati esclusivamente per le seguenti finalità:

- Monitoraggio e sicurezza informatica: garantire l'integrità, la disponibilità e la riservatezza dei sistemi informativi aziendali e prevenire accessi non autorizzati.
- Registrazione e tracciabilità delle attività: registrare e conservare gli accessi logici ai sistemi informatici e agli archivi elettronici per finalità di verifica e controllo, come richiesto dal Provvedimento del Garante Privacy del 27 novembre 2008.
- Eventuale gestione di incidenti di sicurezza e Data Breach: rilevare e segnalare tempestivamente anomalie o violazioni di sicurezza.

La base giuridica del trattamento è l'adempimento di obblighi legali (art. 6, par. 1, lett. c GDPR) in materia di protezione dei dati e sicurezza informatica ovvero l'esercizio di pubblici poteri di cui è investito il Titolare.

4. Tipologia di Dati Raccolti

Nell'ambito delle attività sopra indicate, potranno essere trattati i seguenti dati:

- Dati di accesso (log): username, indirizzo IP, timestamp, azioni eseguite sui sistemi.
- Dati relativi ai dispositivi e connessioni: identificativo del dispositivo, sistema operativo, modalità di accesso (locale o remoto).
- Eventuali segnalazioni di anomalie o tentativi di accesso non autorizzato.

5. Modalità di Trattamento e Sicurezza dei Dati

Il trattamento sarà effettuato con strumenti elettronici e misure di sicurezza adeguate a garantire la protezione, la riservatezza e l'integrità dei dati, tra cui:

- Restrizione degli accessi ai log ai soli soggetti autorizzati.
- Crittografia e sistemi di protezione per prevenire alterazioni o accessi non autorizzati;
- Meccanismi di audit per verificare l'integrità e la correttezza delle registrazioni.

6. Tempi di Conservazione

I dati di log saranno conservati per un periodo non inferiore a **sei mesi**, come previsto dal Provvedimento del Garante Privacy, e comunque per il tempo necessario a garantire la sicurezza dei sistemi e l'adempimento degli obblighi normativi. Decorso tale termine, i dati saranno cancellati o anonimizzati, salvo necessità di conservazione per accertare eventuali

violazioni o per obblighi di legge.

7. Destinatari dei Dati

I dati di log potranno essere accessibili, nei limiti delle rispettive competenze, ai seguenti soggetti:

- Titolare del trattamento e personale autorizzato.
- Responsabile della Protezione dei Dati (DPO) per finalità di controllo e monitoraggio.
- Autorità competenti (es. Garante Privacy, Polizia Postale) in caso di indagini su violazioni di sicurezza.

I dati non saranno diffusi né trasferiti al di fuori dello Spazio Economico Europeo.

8. Diritti dell'Interessato

L'Amministratore di Sistema ha il diritto di:

- Accedere ai propri dati e ottenere informazioni sul loro trattamento.
- Chiedere la rettifica di dati inesatti.
- Opporsi al trattamento, salvo prevalenti obblighi legali del Titolare.
- Chiedere la cancellazione dei dati quando non più necessari o trattati in violazione di legge.

Per esercitare i propri diritti, l'Amministratore può contattare il Titolare o il DPO ai riferimenti suindicati.

9. Reclamo all'Autorità di Controllo

L'Amministratore di Sistema ha il diritto di proporre reclamo al Garante per la Protezione dei Dati Personali se ritiene che il trattamento dei suoi dati violi il GDPR.