S.A.N.B. S.P.A.
Via Mangilli A.C. – 70033 CORATO (BA)
C.F. 07698630725
Numero REA: BA-575480

DETERMINA DELL'AMMINISTRATORE UNICO N. 128/AU DEL 23/03/2021

Oggetto: Atto di nomina dell'Amministratore di Sistema

L'anno 2021, addì 23 del mese di marzo, presso la sede della S.A.N.B. spa sita in Corato (BA) alla via Mangilli A.C., il sottoscritto, **Avv. Nicola Roberto Toscano,** nato a [redacted]), nella sua qualità di **Amministratore unico** della **S.A.N.B. s.p.a..**, cap. soc. Euro 100.000,00 interamente sottoscritto e versato, cod. fisc., p. IVA e numero iscrizione al Registro delle Imprese 07698630725 – in forza della delibera dell'Assemblea straordinaria dei soci del 18/12/2019,

visti:

- il Regolamento UE 679/2016, che d'ora in poi nel presente documento sarà richiamato semplicemente come "GDPR";
- il Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 in G.U. n° 300 del 24 dicembre 2008 che d'ora in poi nel presente documento sarà richiamato semplicemente come "Provvedimento";

considerato che:

- la S.A.N.B. s.p.a. (Servizi Ambientali per il Nord Barese s.p.a.) è una società *in house providing*, interamente partecipata dai Comuni di Bitonto, Corato, Molfetta, Ruvo di Puglia e Terlizzi ed è affidataria del servizio di gestione unitaria di raccolta, smaltimento e trasporto dei rifiuti solidi urbani per i territori dei suddetti Comuni, facenti parte dell'ARO Ba/1;
- il Titolare del Trattamento dei Dati, secondo le prescrizioni del Garante della Privacy del 24 dicembre 2008, è obbligato a designare Amministratori di sistema con competenze tecniche specifiche tali che sia in grado di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio di perdita o violazione dei Dati gestiti;
- per l'attribuzione delle funzioni di Amministratore di sistema occorre indicare l'elencazione analitica degli ambiti di operatività allo stesso consentiti in base al profilo di autorizzazione assegnato;

dato atto che

- per le necessità organizzative aziendali sono stati definiti i seguenti ambiti di operatività:
  - gestione, sicurezza e manutenzione del sistema informatico;
  - gestione sistemistica delle postazioni di lavoro;
  - gestione sistemistica, sicurezza e monitoraggio della rete informatica;
  - gestione sistemistica dei Server aziendali;
  - back-up e Disaster Recovery;
  - gestione dei sistemi software e delle basi dati relative agli applicativi in uso;

valutato

- il curriculum professionale del candidato dott. Nicola D'Introno da cui emerge una accertata esperienza nel settore ed una adeguata formazione professionale in relazione all'attribuzione della nomina di Amministratore di Sistema, in aggiunta alle mansioni di normale assegnazione come rientranti nel profilo professionale di appartenenza;
- la capacità e l'affidabilità tecnica sotto il profilo della sicurezza, dichiarate e garantite dal candidato;

tenuto conto di tutto quanto innanzi esposto

DETERMINA

di **dare atto** che quanto specificato in premessa è parte integrante del dispositivo del presente atto;

di nominare quale Responsabile di Sistema secondo il Provvedimento del Garante della Privacy del 24 dicembre 2008 il dott. Nicola D'Introno, dipendente di Sanb SpA;

di definire gli ambiti di operatività del Responsabile di Sistema, come segue:

a. gestione, sicurezza e manutenzione del sistema informatico;
b. gestione sistemistica delle postazioni di lavoro;
c. gestione sistemistica, sicurezza e monitoraggio della rete informatica;
d. gestione sistemistica dei Server aziendali;
e. back-up e Disaster Recovery;
f. gestione dei sistemi software e delle basi dati relative agli applicativi in uso.

di definire i compiti affidati in:

- progettazione, installazione, configurazione, gestione e manutenzione dei sistemi informatici;
- controllo sul corretto utilizzo, funzionamento e protezione dei sistemi di gestione ed elaborazione dei dati;
- impostazione e gestione dei sistemi di autenticazione e di autorizzazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
- organizzazione e gestione dei flussi di rete;
- gestione dei supporti di memorizzazione;
- manutenzione dell'hardware;
- classificazione analitica delle banche dati ed impostazione/organizzazione di un sistema complessivo di trattamento informatizzato dei dati personali comuni e particolari, nel rispetto della normativa vigente in materia di protezione dei dati personali;
- predisposizione e gestione dei sistemi di salvataggio (backup), anche automatici, con adozione di adeguate procedure per la custodia delle copie di sicurezza dei dati;
- adozione di adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS ecc.);
- predisposizione di sistemi di ripristino dei dati e dei sistemi (recovery), anche automatici, che assicurino di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- adozione di un sistema idoneo alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici; 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 dodici mesi;
- adozione di tutte le misure di sicurezza adeguate al rischio, ivi comprese:
  - la pseudonimizzazione e la cifratura dei dati personali;
  - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento;
- adozione delle misure di sicurezza ICT emanate dall'AgID, adeguate alla realtà organizzativa aziendale;
- verifica e monitoraggio costante dei sistemi informatici al fine di rilevare immediatamente 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;
- controllo sugli interventi informatici effettuati da operatori esterni;
- predisposizione di un piano di controlli periodici, da eseguire con cadenza almeno semestrale, atti a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- provvedere alla distruzione e smaltimento dei supporti informatici di memorizzazione logica obsoleti e/o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento dei dati personali;

di trasmettere copia del presente provvedimento al Collegio sindacale, anche nella sua funzione di OdV, al Revisore contabile, al Responsabile della prevenzione della corruzione e della trasparenza di S.A.N.B. s.p.a., nonché ai soci anche nell'ambito delle rispettive prerogative di controllo analogo.

L'amministratore Unico
Avv. Nicola Roberto Toscano