UNIONE TERRED'ACQUA

Costituita fra i Comuni di:

Anzola dell'Emilia
Calderara di Reno
Crevalcore
Sala Bolognese
San Giovanni in Persiceto
Sant'Agata Bolognese

DECRETO DEL PRESIDENTE

DECRETO DEL PRESIDENTE NR. 28
DEL 30/10/2018

OGGETTO:
DECRETO DI NOMINA DELL'AMMINISTRATORE DEL SISTEMA INFORMATICO DELL'UNIONE TERRED'ACQUA

Soggetti destinatari:
VENTURA ANDREA

PRESIDENTE

BASSI EMANUELE

Documento prodotto in originale informatico e firmato digitalmente ai sensi dell'art. 20 del "Codice dell'amministrazione digitale" (D.Leg.vo 82/2005).

DECRETO NR. 28 DEL 30/10/2018

OGGETTO:
DECRETO DI NOMINA DELL'AMMINISTRATORE DEL SISTEMA INFORMATICO DELL'UNIONE TERRED'ACQUA

IL PRESIDENTE DELL'UNIONE

Visto il Regolamento Ue 2016/679 del Parlamento europeo e del Consiglio datato 27 aprile 2016 "Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. (Regolamento generale sulla protezione dei dati), entrato in vigore il 24 aprile 2016 e da applicare a decorrere dal 25 maggio 2018;

Visto il D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", come novellato dal D.Lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679;

Visto il provvedimento del Garante della Privacy datato 27 novembre 2008 dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008, come modificato con successivo provvedimento del 25 giugno 2009;

Visto il D. Lgs. 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" e ss.mm.ii.;

Dato atto che l'Unione Terre d'Acqua è Titolare del trattamento dei dati personali effettuato anche con strumenti elettronici necessario per lo svolgimento dei procedimenti amministrativi afferenti alle funzioni istituzionali affidate dalle fonti di diritto dell'Unione europea e dello Stato italiano;

Visto il paragrafo 1 dell'art. 32 del Regolamento UE 2016/679 il quale prescrive che *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio."*

Tenuto conto che il legislatore europeo ha previsto un nucleo minimo di misure, da attuare prima del trattamento e sin dalla progettazione delle modalità di svolgimento dello stesso trattamento, che rispondono a criteri di sicurezza predefiniti e che sono dirette a bilanciare in maniera adeguata il rischio a contrasto del quale sono definite, tra le quali molto rilevanti risultano essere:

- 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 e organizzative al fine di garantire la sicurezza dei dati personali;

DECRETO NR. 28 DEL 30/10/2018

Atteso che il sig. Andrea Ventura, dipendente dell'Unione Terre d'Acqua a tempo indeterminato, inquadrato nella categoria "D3", ha la verificata idoneità ad assumere l'incarico di Amministratore del Sistema della rete e delle postazioni di lavoro informatizzate, essendo in possesso di tutte le caratteristiche di esperienza, capacità e affidabilità nonché di moralità richieste dalle vigenti disposizioni per adempiere ai compiti in materia di sicurezza del trattamento informatico dei dati, e per svolgere attività di gestione tecnica del sistema informatico;

Visto lo Statuto dell'Unione Terre d'Acqua;

Visto il D. Lgs. 18 agosto 2000, n. 267;

NOMINA

il sig. Andrea Ventura , nato a Casalecchio di Reno il 15 ottobre 1961, dipendente a tempo indeterminato di questo Ente e inquadrato nella categoria "D3", quale Amministratore del sistema informatico di questo Ente, il quale é tenuto svolgere tutti gli adempimenti necessari sia sul piano delle procedure amministrative, che dell'organizzazione, che dell'adozione e verifica di ogni misura tecnica e organizzativa necessaria in materia di sicurezza per la protezione dei dati personali in conformità: alle disposizioni normative di cui alle fonti di diritto dell'Unione europea e dello Stato italiano; ai provvedimenti e alle direttive impartite dal "Gruppo di Lavoro europeo 29" e dal Garante della Privacy; alle disposizioni regolamentari e alle direttive emanate dal Titolare del trattamento e dal Responsabile della protezione dei dati di questo Ente; alla disciplina del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82/2004 e ss.mm.ii..

L'Amministratore del sistema informatico svolge in particolare la cura dei seguenti adempimenti:

a) gestire l'hardware e i software dei server della rete e delle postazioni di lavoro informatizzate;
b) impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
c) registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema; impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per i Responsabili e gli Incaricati dei trattamenti di dati personali effettuati con strumenti elettronici nonché di quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzati;
d) verificare costantemente che il Titolare del trattamento abbia adottato le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, provvedendo senza indugio agli adeguamenti eventualmente necessari, redigendo entro il 30 settembre di ogni anno una apposita relazione da inviare al Sindaco, al Segretario Generale e al Responsabile per la protezione dei dati in modo da attuare gli adempimenti amministrativi e contabili per la previsione nella successiva programmazione utile per la realizzazione delle ulteriori misure;
e) suggerire al Titolare del trattamento, ai Designati del trattamento l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati atte a che i dati personali oggetto di trattamento siano 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;

Più specificamente, l'Amministratore di sistema dovrà:

1) assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nel Disciplinare tecnico e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti e alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare ai Responsabili e agli Incaricati del trattamento dei dati, svolgendo anche la funzione di custode delle copie delle credenziali; Più specificamente dovrà:
   - custodire le parole chiave attribuite dagli incaricati del trattamento di dati personali con elaboratori elettronici e preservare con estrema attenzione il "cartellino delle credenziali di autenticazione" in modo da evitare accidentali aperture della busta ed evitare di aprire tali buste;
   - nel caso in cui il Designato del trattamento abbia la necessità indifferibile di accedere ad un elaboratore in caso di assenza o impedimento dell'incaricato che lo utilizza abitualmente, consentire al Designato del trattamento con una nuova parola chiave l'accesso all'elaboratore sul quale egli possa intervenire unicamente per necessità di operatività e sicurezza del sistema informativo; informare l'Incaricato del trattamento allorché rientri in servizio e consegnargli una nuova parola chiave diversa da quella consegnata al Designato del trattamento durante la sua assenza.
2) procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva ai soggetti interessati l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;
3) dotare e attivare nonché aggiornare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza e protezione dei dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici, ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi;
4) aggiornare periodicamente, con frequenza almeno annuale (oppure semestrale se si trattano dati sensibili o giudiziari), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
5) curare l'adozione e l'aggiornamento delle predette misure di sicurezza;
6) impartire a tutti i soggetti che comunque svolgano trattamento dei dati istruzioni organizzative dirette al salvataggio quotidiano dei dati; prendere pertanto tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up; assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
7) adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
8) predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza;
9) indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati allorché si provveda al loro reimpiego;

All'Amministratore del sistema informatico è :

a) fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati; tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Designati del trattamento a conoscere i dati personali oggetto di trattamento;
b) obbligato a dare tempestiva comunicazione al Titolare e ai Designati del trattamento interessati nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati;
c) obbligato a osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici, degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta dei dati.

Nell'espletamento dell'incarico conferito, l'Amministratore del sistema informatico è tenuto ad osservare ed applicare le seguenti disposizioni:

- sovrintendere alle risorse del sistema operativo di base dati e consentirne l'utilizzazione;
- vigilare sul corretto funzionamento di tutti i componenti del sistema informatico, per evitare problemi di perdita o danneggiamento di dati personali;
- verificare che siano adottati tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati;
- controllare che siano eseguiti salvataggi periodici dei dati con copie di backup;
- assicurarsi della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
- decidere se i supporti di backup sono riutilizzabili, in questo caso, con quale modalità e periodicità;
- proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus informatici mediante idonei programmi;
- attribuire a ciascun incaricato del trattamento le credenziali univoche di autenticazione composte da codice per l'identificazione dell'incaricato e password per l'utilizzazione del sistema e, dove previsto, dei singoli applicativi o sistemi componenti; le password dovranno essere composte, ove tecnicamente possibile, da almeno otto caratteri; uno stesso codice non può, neppure in tempi diversi, essere riassegnato a persone diverse;
- assistere il titolare ed i designati dei trattamenti nell'attuazione pratica delle misure e indicazioni previste dal diritto dell'Unione e dello Stato, in particolare all'attuazione dei vincoli sulle operazioni previsti per il singolo profilo di autorizzazione;
- cancellare i dati contenuti nei supporti di memorizzazione una volta terminato la necessità di conservazione e, nell'impossibilità, procedere alla distruzione fisica dei supporti;
- limitare l'intervento solamente secondo le modalità e misura strettamente necessarie ad adempiere alle operazioni di manutenzione dei programmi o del sistema informatico;
- vigilare durante gli interventi in loco sull'applicazione delle procedure ed istruzioni definite; in caso di necessità trasferire al fornitore le apparecchiature elettroniche, parti di esse o supporti contenenti i dati oggetto della manutenzione; se l'oggetto della manutenzione non sono i dati stessi o il loro recupero, e se tecnicamente possibile i supporti di registrazione devono essere cancellati prima dell'asporto (verificando se é necessario effettuare un backup). Ove prevista, la password di accesso sarà comunicata al fornitore provvedendo a cambiarla al termine delle operazioni di manutenzione.

DECRETO NR. 28 DEL 30/10/2018

Il Dirigente del settore “Affari Generali” provvede, tempestivamente, a che i dati identificativi e di contatto dell’Amministratore del sistema informatico siano pubblicati nel sito web istituzionale dell’Ente.

Il Responsabile della protezione dei dati procederà, entro il mese di settembre di ogni anno, alla verifica delle attività svolte dall’Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

IL PRESIDENTE DELL’UNIONE

EMANUELE BASSI

(documento firmato digitalmente)