



COMUNE DI RIVA DEL GARDA

Numero di protocollo associato al documento come metadato (DPCM 3.12.2013 n. 20). Data di registrazione inclusa nella segnatura di protocollo.

DECSIRE0600072

Nomina ad Amministratore di sistema – dott.ssa Michela Piva Responsabile dell’U.O. Sistema Informativo Comunale.

(Artt. 28 e 32 del Regolamento europeo sul trattamento dei dati personali n 679/2016 e Provvedimento a carattere generale del Garante per la protezione dei dati personali di data 27 novembre 2008)

IL TITOLARE

Visto il Regolamento europeo sulla protezione dei dati 27 aprile 2016, n. 679;

visto il decreto legislativo 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali” come modificato dal decreto legislativo 8 agosto 2018, n. 101;

visto il Provvedimento a carattere generale del Garante per la protezione dei dati personali di data 27 novembre 2008, avente ad oggetto “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”;

vista la Circolare dell’Agenzia per l’Italia Digitale (AgID) 18 aprile 2017, n. 2, che detta le misure minime di sicurezza ICT per le Pubbliche Amministrazioni nel rispetto del Codice per l’Amministrazione Digitale;

considerato che per capacità, esperienza ed affidabilità la dott.ssa Michela Piva, dipendente del Comune di Riva del Garda e responsabile dell’U.O. Sistema Informativo Comunale, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nel trattamento dei dati personali;

richiamato il decreto del Sindaco pro tempore di data 27 marzo 2009 (prot. n. 0010221 di pari data) con il quale la dott.ssa Michela Piva è stata nominata amministratore di sistema dell’ente;

rilevata la necessità di aggiornare i contenuti del precitato provvedimento di nomina per adeguarli alle disposizioni vigenti;

visto il Codice degli Enti Locali della Regione autonoma Trentino-Alto Adige approvato con Legge regionale 3 maggio 2018 n. 2;

visto lo Statuto;

visto il Regolamento organico del personale;

NOMINA

la dott.ssa Michela Piva,
AMMINISTRATORE DI SISTEMA

PER LA GESTIONE E MANUTENZIONE DEL SISTEMA INFORMATICO

del Comune di Riva del Garda

In relazione a tale incarico Lei ha il compito di sovrintendere e gestire le risorse del sistema informativo e del sistema di basi di dati dell'Ente, in base alle prescrizioni e indicazioni date dal Titolare.

In qualità di amministratore di sistema **Lei può accedere e effettuare il trattamento dei dati gestiti nel sistema informatico unicamente per finalità di gestione, manutenzione e limitando le operazioni a quelle necessarie a tali fini, trattando i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle operazioni di manutenzione in modo lecito, con assoluta riservatezza e secondo correttezza.**

In particolare, nell'effettuare operazioni di gestione e manutenzione:

- se è necessario eseguire stampe per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, quando non strettamente necessario relativamente al test in oggetto, deve utilizzare files di prova privi di dati personali;
- eventuali stampe di prova di dati personali vanno immediatamente distrutte, così come vanno cancellate o restituite le registrazioni di dati personali su supporti di registrazione;
- se è strettamente necessario accedere a files già esistenti contenenti dati personali (ad esempio files di log o per il recupero di un testo) trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle operazioni di manutenzione in modo lecito e secondo correttezza ed ai soli fini della gestione e manutenzione;
- se è strettamente necessario accedere alle caselle istituzionali di posta elettronica (ad esempio per interventi di assistenza richiesti dal personale dipendente o per interventi di chiusura forzata di caselle istituzionali di dipendenti cessati) trattare tutti i dati personali di cui si viene incidentalmente a conoscenza nell'ambito dello svolgimento delle operazioni di manutenzione in modo lecito e secondo correttezza ed ai soli fini della gestione e manutenzione. Ogni accesso effettuato dagli amministratori di sistema alle caselle istituzionali di posta elettronica viene automaticamente tracciato dal sistema che rileva il nominativo dell'amministratore di sistema, la data, l'ora di accesso e la casella di posta elettronica interessata;
- se vi è necessità Le è consentito prelevare e trasferire presso il Suo centro di assistenza tecnica apparecchiature elettroniche, parti di esse o supporti contenenti i dati oggetto della manutenzione ed assistenza. Se l'oggetto della manutenzione ed assistenza 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 è necessario o utile consegnare un backup agli addetti). Ove prevista, la password di accesso è comunicata dall'incaricato il quale provvede a cambiarla al termine

delle operazioni di manutenzione;

- i dati sono consegnati al solo fine della manutenzione ed assistenza e non devono essere utilizzati per scopi diversi da quelli per i quali è stato richiesto l'intervento;
- l'accesso per la tele-assistenza deve avvenire esclusivamente se motivato da oggettive necessità dipendenti dall'oggetto dell'incarico e richiede che l'incaricato attivi il programma che consente la tele-assistenza.

È suo compito implementare una **misura idonea alla registrazione degli accessi** da Lei compiuti al sistema informativo (access log), che comprenda i riferimenti temporali e la descrizione dell'evento e che consenta di conservare tali registrazioni in maniera completa e inalterata per un periodo minimo di sei mesi.

Collaborando con il Titolare del trattamento, deve osservare e adempiere alle seguenti prescrizioni:

- impostare e gestire un **sistema di autenticazione informatica** per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dall'art. 32 del Regolamento europeo 679/2016; in particolare, deve:
 1. 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;
 2. prevedere password composte, ove tecnicamente possibile, da almeno otto caratteri;
 3. prevedere che uno stesso codice non possa, neppure in tempi diversi, essere riassegnato a persone diverse;
 4. prevedere un sistema che obblighi gli incaricati alla modifica delle credenziali univoche di autenticazione con una cadenza trimestrale;
 5. operare la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi o in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- impostare e gestire un **sistema di autorizzazione informatica** per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme dall'art. 32 del Regolamento europeo 679/2016; in particolare deve:
 1. configurare d'intesa con il titolare un sistema di autorizzazione;
 2. configurare i profili di autorizzazione degli incaricati e dei responsabili prima dell'inizio del trattamento;
 3. periodicamente e almeno annualmente verificare le condizioni per la conservazione dei profili di autorizzazione da parte degli incaricati e dei responsabili
 4. verificare costantemente che l'Ente abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dalla Circolare dell'Agenzia per l'Italia Digitale (AgID) 18 aprile 2017, n. 2, che detta le misure minime di sicurezza ICT per le Pubbliche Amministrazioni nel rispetto del Codice per l'Amministrazione Digitale provvedendo senza indugio agli adeguamenti eventualmente necessari;
- suggerire **l'adozione e l'aggiornamento delle misure di tecniche e organizzative adeguate** a garantire il livello di sicurezza adeguato al rischio atte a realizzare quanto previsto all'art. 32 del Regolamento europeo 679/2016;
- curare **l'adozione e l'aggiornamento delle eventuali misure adeguate** di cui al punto precedente;
- attivare e aggiornare idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici;
- aggiornare periodicamente i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;

- adottare procedure per la **custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi (operazioni di backup e recovery dei dati)**;
- predisporre un piano di controlli periodici, da eseguirsi con cadenza annuale, dell'efficacia delle misure di sicurezza adottate.

È Suo compito riferire periodicamente, ed in ogni caso con cadenza **almeno annuale** al Titolare sullo svolgimento dei Suoi compiti, mediante presentazione di **dettagliata relazione degli interventi effettuati corredata dalla dimostrazione necessaria per dimostrare conformità a tutti i suoi obblighi**.

È tenuto a fornire piena collaborazione al Titolare nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.

È tenuto ad assistere il Titolare nell'adempimento dell'obbligo di rispondere alle richieste di esercizio dei diritti degli interessati e delle istanze del Garante per la protezione dei dati personali.

Il presente atto sostituisce integralmente l'atto di nomina di data 27 marzo 2009 prot. n. 0010221.

IL SINDACO
f.to dott.ssa Cristina Santi

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (art. 3 bis e 71 D.Lgs. 82/2005). L'indicazione a stampa del nominativo del firmatario sostituisce la sua firma autografa (art. 3 D.Lgs 39/1993).

ks – s.

L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D.Lgs. 39/1993).
L'originale firmato digitalmente è depositato presso l'ufficio Segreteria Organizzativa.