COMUNE DI SALTRIO

Provincia di Varese

Via Cavour n. 37 – 21050 Saltrio (VA) * Tel.n. 0332/486166 – Fax n. 0332/486178
sito internet: www.comune.saltrio.va.it * E-mail: saltrio@comune.saltrio.va.it
P.E.C.: comune.saltrio.va@legalmail.it – Codice fiscale/P. I.V.A. 00560460123

DECRETO DEL SINDACO
n. 000013 del 23.04.2019

OGGETTO: ATTO DI NOMINA AUTORIZZATO AL TRATTAMENTO AI SENSI DEL REGOLAMENTO UE 2016/679 GENERAL DATA PROTECTION REGULATION (GDPR) - ZAPPIERI PAOLA.

IL SINDACO

quale legale rappresentante pro tempore del Comune di Saltrio in qualità di *"Titolare del Trattamento"* dei dati personali, ai sensi e per gli effetti dell' art. 29 del GDPR, con il presente atto

N O M I N A

la dipendente di ruolo sig.ra **Paola ZAPPIERI**, inquadrata nella categoria C, quale **AUTORIZZATA al trattamento dei dati personali**.

Tale nomina è in relazione alle operazioni di elaborazione di dati personali ai quali i soggetti Autorizzati hanno accesso nell'espletamento della funzione che è loro propria. In particolare non è consentito l'accesso a dati la cui conoscenza non è necessaria all'adempimento dei compiti affidati agli Autorizzati.

In ottemperanza a quanto previsto dal GDPR, costituisce trattamento dei dati personali *"qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati"*.

L'ambito di applicazione della presente nomina fa riferimento ai tipi di dati ed alle mansioni sotto elencate.

L'Autorizzato al trattamento dei dati personali è tenuto a:

- ✓ procedere alla raccolta di dati personali, comprensiva anche dell'informativa sul trattamento dei dati personali;
- ✓ trattare i dati personali nella misura necessaria e sufficiente alle proprie finalità;
- ✓ adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal Titolare del trattamento, in particolare:
- ✓ custodire con attenzione le proprie credenziali di autenticazione ed ogni dispositivo che la contiene, evitare di operare su terminali altrui, lasciare accessibile il proprio terminale in caso di allontanamento, anche temporaneo, dal posto di lavoro, al fine di evitare trattamenti non autorizzati;
- ✓ trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
- ✓ conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che siano accessibili a persone non autorizzate al trattamento dei dati medesimi o siano facilmente oggetto di danneggiamenti intenzionali o accidentali;
- ✓ effettuare copie di dati personali oggetto di trattamento esclusivamente se necessario e soltanto previa autorizzazione del Titolare del trattamento;
- ✓ avvisare immediatamente il Titolare del trattamento in caso si constati o si sospetti un incidente di sicurezza;
- ✓ segnalare al titolare del trattamento eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- ✓ mantenere la riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- ✓ svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal Titolare del trattamento e, comunque, in modo lecito.

Il presente incarico è strettamente collegato e funzionale alle mansioni svolte da ciascun Autorizzato e necessario per lo svolgimento delle stesse, pertanto non costituisce conferimento di nuova mansione o ruolo.

L'Autorizzato dichiara di aver ricevuto le adeguate istruzioni e si impegna, dopo averne presa visione, ad adottare tutte le misure necessarie alla loro attuazione.

L'Autorizzato dovrà osservare scrupolosamente tutte le istruzioni ricevute e le misure di sicurezza già in atto o che verranno eventualmente comunicate in seguito dal Titolare del trattamento.

L'accettazione del presente atto di nomina costituisce consapevole accettazione degli obblighi assunti.

ISTRUZIONI PER L'AUTORIZZATO

L'art. 29 Reg. UE 2016/679 definisce come autorizzati *"le persone fisiche che sotto la responsabilità di un Titolare o di un Responsabile agiscono accedendo a dati personali"*.

Nell'ambito di competenza a lei assegnato dal Titolare nell'atto di nomina, vengono sotto riportate le istruzioni a cui è tenuto ad attenersi nel trattamento di dati personali, in conformità alle normative vigenti sulla Privacy.

PROCEDURE PER LA CLASSIFICAZIONE DEI DATI.

L'Autorizzato deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge. Qualora non fosse in grado, deve fare riferimento al Titolare del Trattamento.

La natura dei dati trattati:

- ✓ *«dato personale»*: qualsiasi informazione riguardante una persona fisica identificata o identificabile (*«interessato»*); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- ✓ *«dati genetici»*: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- ✓ *«dati biometrici»*: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare: non trattare nessun documento al di fuori delle autorizzazioni ricevute.

Gli atti o i documenti contenenti dati personali non devono mai essere lasciati incustoditi o privi di controllo: occorre pertanto dotarsi di adeguati strumenti di sicurezza, come cassetti con serratura o altri accorgimenti aventi funzione equivalente, nei quali riporli.

E' sempre necessario ricorrere a tali strumenti prima di assentarsi dal posto di lavoro, anche per assenze di breve durata, in modo particolare se i documenti trattati contengono dati sensibili o giudiziari.

L'accesso ai documenti è consentito solo al personale espressamente autorizzato e al termine del trattamento svolto è necessario archiviarli seguendo tassativamente le regole di archiviazione dell'Ente.

REGOLE DI UTILIZZO DEL SISTEMA INFORMATICO COMUNALE

Definizioni

Sistema Informatico Comunale (di seguito S.I.C.): l'insieme degli strumenti tecnologici utilizzati dal Comune per il trattamento e la conservazione delle informazioni, composto dalle singole postazioni di lavoro, da elementi hardware (server di rete, stampanti, periferiche, ecc.), software (programmi informatici di base e applicativi, database, ecc.) e reti telematiche.

Amministratore di Sistema (AdS): figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione dati, all'amministrazione di basi di dati, di reti, di apparati di sicurezza e di sistemi software complessi.

Utente: persona che a qualsiasi titolo accede, anche in forma parziale o per limitati periodi di tempo, al S.I.C..

Informazioni e norme generali.

Gli Utenti del S.I.C. sono formalmente autorizzati dall'Amministrazione e tecnicamente abilitati dal AdS, non è consentito alcun accesso anonimo o non autorizzato.

Ogni utente è tenuto ad osservare le presenti regole al fine di preservare la funzionalità e la sicurezza del sistema stesso e delle informazioni gestite e conservate.

Gli strumenti informatici possono essere utilizzati unicamente per gli scopi definiti dall'Amministrazione.

Norme tecniche

Postazioni di lavoro

Ogni postazione di lavoro si compone di:
- ✓ dotazione hardware e software
- ✓ impostazioni utente (salvaschermo, memorizzazione password, ecc.)
- ✓ autorizzazione per l'accesso a cartelle condivise e software applicativi

Qualsiasi variazione alla configurazione della postazione di lavoro (ad esempio l'installazione di nuovi software o la rimozione o aggiornamento di quelli presenti, l'utilizzo di USB drive o altri supporti informatici, la modifica delle impostazioni utente, ecc.) deve essere preventivamente autorizzata dal Responsabile di servizio e concordata con l'AdS.

Non è consentito il collegamento al S.I.C. di apparecchiature non di proprietà dell'Amministrazione, salvo specifica autorizzazione del AdS.

Credenziali utente

Ciascun utente del S.I.C. si connette alla rete, alle piattaforme software e alla posta elettronica, tramite autenticazione univoca personale. L'utente è tenuto a custodire e garantire la segretezza della parola chiave e a sostituirla almeno ogni sei mesi.

Le password sono modificabili da tutti gli utenti in qualsiasi momento tramite apposita procedura, specifica di ogni contesto applicativo.

I requisiti minimi di complessità delle password sono:
- ✓ redazione con caratteri maiuscoli e minuscoli
- ✓ composizione con inclusione di lettere, numeri e simboli o segni di punteggiatura
- ✓ numero caratteri non inferiori ad 8
- ✓ password non agevolmente riconducibile all'identità del soggetto che la gestisce

Gestione dei dati

La rete interna, istituita appositamente per permettere collegamenti funzionali tra gli utenti, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.

Le cartelle di rete sono sottoposte a procedure di backup e controllo degli accessi e sono l'unico supporto sicuro sul quale memorizzare i documenti elettronici. L'utilizzo da parte degli utenti di qualsiasi altro supporto di memorizzazione (ad esempio le cartelle locali del personal computer) non garantisce la sicurezza del dato in caso di guasti hardware, sovrascritture o cancellazioni accidentali, attacchi informatici di virus o altri software malevoli.

Qualsiasi file estraneo all'attività lavorativa, se non espressamente autorizzato, non può,

nemmeno in via transitoria, essere salvato nelle cartelle di rete.

Tutti i file di provenienza incerta o comunque esterna (Internet, posta elettronica, supporti rimuovibili), ancorché attinenti l'attività lavorativa, devono essere sottoposti al controllo antivirus.

E' vietata la cifratura di documenti effettuata autonomamente dall'utente se non concordata e autorizzata dal ADS.

Utilizzo rete Internet

L'accesso a Internet è possibile da qualsiasi postazione connessa alla rete e costituisce parte integrante della dotazione informatica di ogni utente.

Non è consentito l'accesso a siti, social network o qualsiasi altro tipo di risorsa on-line, per scopi non inerenti la propria attività lavorativa, salvo autorizzazione concordata con l'Amministrazione Comunale.

Il S.I.C. può impiegare sistemi automatici di filtraggio degli indirizzi Internet per impedire l'accesso da parte degli utenti a siti di carattere non istituzionale.

L'Amministrazione Comunale può inoltre avvalersi di sistemi in grado di documentare il traffico internet generato dalla stazioni di lavoro. Tali informazioni sono raccolte unicamente allo scopo di verificare ex-post utilizzi illeciti del collegamento ad Internet e il loro accesso è consentito unicamente al Titolare del trattamento dati personali e si effettuerà unicamente nei modi previsti dalla legge ed in particolare secondo principi di gradualità dei controlli, pertinenza e non eccedenza.

Utilizzo posta elettronica

Tutte le caselle appartenenti al dominio istituzionale, comprese pertanto anche quelle nominali, sono di esclusiva proprietà dell'Amministrazione Comunale e il loro utilizzo è autorizzato solo per esigenze di servizio.

Lo strumento della posta elettronica non sostituisce altri sistemi più idonei per l'interscambio di documenti, pertanto l'invio di allegati è consentito solo per file con dimensioni contenute (fino a un massimo di 25 Mb).

In caso di assenza programmata o prolungata, ogni utente dispone di apposite funzioni automatiche di sistema che consentono di inviare messaggi di risposta o inoltrare la posta verso differenti indirizzi.

Protezione antivirus

Ogni utente è tenuto a tenere comportamenti tali da ridurre il rischio di attacco al S.I.C. da parte di virus o di ogni altro software malevolo che operi con lo scopo di superare le difese di sicurezza del sistema stesso.

A tal fine, ogni utente è tenuto a:

- ✓ evitare tassativamente l'apertura di file allegati ad e-mail provenienti da utenti sconosciuti o contenenti messaggi sospetti
- ✓ segnalare tempestivamente all'AdS eventuali avvisi di rischio ricevuti dal software antivirus installato o altre anomalie di funzionamento del sistema
- ✓ evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile
- ✓ evitare l'utilizzo di dispositivi rimuovibili (USB drive, CD/DVD, floppy disk o simili) personali o non autorizzati dall'AdS

- ✓ controllare, mediante il software antivirus, il contenuto di supporti rimuovibili autorizzati prima di ogni utilizzo.

Accesso ad archivi contenenti dati personali

Il Comune di Saltrio, per perseguire le proprie finalità istituzionali, gestisce archivi contenenti dati personali tutelati dalla normativa in materia di Privacy.

L'accesso agli archivi contenenti dati personali (comuni e/o sensibili) è consentito esclusivamente agli utenti autorizzati, identificati tramiti le proprie credenziali di accesso al sistema.

Ogni utente è tenuto a non allontanarsi dal proprio posto di lavoro senza aver prima chiuso la propria sessione di lavoro o bloccato in altro modo l'accesso non autorizzato al proprio sistema.

Notifica, comunicazione e pubblicazione del presente decreto

A cura del Segretario Generale, il presente decreto è notificato al sopra designato Responsabile del trattamento; comunicato al Responsabile della protezione; pubblicato nella sezione *"Amministrazione trasparente – altri contenuti – Privacy"* del sito web istituzionale di questo Comune.

IL SINDACO
ing. Maurizio Zanuso

Firmato da:
MAURIZIO ZANUSO
Codice fiscale: ZNSMRZ59T23D869F
Organizzazione: NON PRESENTE
Valido da: 08-03-2018 11:44:05 a: 08-03-2021 02:00:00
Certificato emesso da: InfoCert Firma Qualificata 2, INFOCERT SPA, IT
Riferimento temporale 'SigningTime': 23-04-2019 16:47:24
Approvo il documento