Originale

COMUNE DI BARESSA

Provincia di Oristano

DECRETO DEL SINDACO

N.11 del 04/06/2021

OGGETTO:

DECRETO DI NOMINA DELLE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI, EFFETTUATO MEDIANTE IL SISTEMA DI VIDEOSORVEGLIANZA COMUNALE AI SENSI DELL'ART. 2 QUATERDECIES, COMMA 2, DEL D. LGS. N. 196/2003 E SS. MM. II.

*L'anno **2021** addì **quattro** del mese di **Giugno** , nella sede comunale,*

Il Sindaco, nella sua qualità di legale rappresentante dell'Ente

PREMESSO CHE:

- **in data 25 maggio 2018**, è divenuto definitivamente applicabile in via diretta in tutti i Paesi UE il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 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)»* (di seguito *RGPD*);
- in data 10 agosto 2018 è stato adottato il D. Lgs. 101/18, entrato in vigore il 19 settembre 2018, di modifica del D. Lgs. 196/03 recante disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 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)»*;
- ai sensi dell'art.4, paragrafo 1, punto 7), RGPD 2016/679, per **Titolare del trattamento** si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o l'organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. **Nel caso di una Pubblica Amministrazione, il Titolare del trattamento dei dati è l'Ente nel suo complesso**;
- l'art. 2 *quaterdecies*, comma 2, del D. Lgs. n. 196/2003 aggiornato al D. Lgs. n. 101/2018, stabilisce che il Titolare del trattamento individua "*le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*";

- In data 26 luglio 2018 con Delibera di C.C. n. 18 del 26.07.2018 l'Ente ha adottato il Regolamento comunale sulla Videosorveglianza;
- le persone fisiche autorizzate, effettueranno il trattamento dei dati, attenendosi scrupolosamente alle istruzioni impartite dal Titolare del trattamento
- Si rende necessario procedere alla formale ed espressa individuazione delle persone fisiche all'Ente che saranno autorizzate al trattamento dei dati personali nell'ambito dell'Area Amministrativa/Finanziaria con particolare riferimento alle Banche Dati relative al Sistema di gestione della VIDEOSORVEGLIANZA al fine della puntuale individuazione dell'ambito di trattamento loro consentito;

tutto ciò premesso

DECRETA

di designare quali persone autorizzate al trattamento dei dati personali necessari per l'espletamento delle procedure relative alla gestione del **sistema di Videosorveglianza** i Signori:

Ass.te Sc. P.L. COMINA ENZO – UFFICIO POLIZIA LOCALE –

che, in relazione ai compiti loro affidati, vengono a contatto, nelle diverse fasi dell'attività, con tali informazioni.

In ottemperanza al RGPD, che disciplina la protezione delle persone fisiche con riferimento al trattamento dei dati personali, le SS. LL. sono autorizzate a trattare i dati personali, nonché le eventuali categorie particolari di dati di cui agli artt. 9 e 10 del RGPD, strettamente necessari per l'espletamento delle fasi procedimentali di competenza, **con riferimento alla gestione del Sistema di Videosorveglianza,** secondo le indicazioni di seguito dettagliate.

I dipendenti, individuati quali Autorizzati al trattamento dovranno:

- trattare i dati personali di cui vengano a conoscenza nell'ambito dello svolgimento della propria attività in modo lecito e secondo correttezza;
- effettuare le operazioni di trattamento di cui al RGPD esclusivamente per lo svolgimento delle funzioni istituzionali legate alla gestione del Sistema Comunale di Videosorveglianza;
- accedere unicamente alle banche dati strettamente necessarie per l'espletamento di funzioni istituzionali nell'ambito della gestione del Sistema di Videosorveglianza in ossequio alle previsioni contenute nel vigente Regolamento Comunale sulla Videosorveglianza adottato con Deliberazione del C.C. n. 20 del 26.07.2021 che qui si richiama integralmente;
- per le banche dati informatiche, utilizzare sempre le proprie credenziali di accesso personali, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- mantenere la massima riservatezza ed il dovuto riserbo sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali con riferimento alla gestione del Sistema di Videosorveglianza comunale;

- custodire e controllare i dati personali affidati affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare banche dati nuove senza autorizzazione espressa del Dirigente/Titolare di PO;
- conservare i dati rispettando le misure di sicurezza predisposte dall'Ente;
- fornire al Dirigente/Titolare di PO dei dati tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo.

Con riferimento all'utilizzo della postazione di lavoro assegnata in uso per l'espletamento di funzioni istituzionali nell'ambito della gestione del Sistema di Videosorveglianza:

- Il Personal Computer (PC) affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente l'attività lavorativa può contribuire ad innescare disservizi, costi ulteriori di manutenzione e minacce alla sicurezza dei dati personali trattati dall'Ente.
- I dipendenti devono custodire la propria strumentazione in modo diligente, segnalando con tempestività ogni danneggiamento, avaria, furto o smarrimento al Titolare del trattamento.
- L'accesso a ciascun PC è protetto da credenziale di autenticazione costituita da una User ID (codice per l'identificazione dell'autorizzato) associata a una PASSWORD riservata (parola chiave), conosciuta esclusivamente dal medesimo autorizzato.
- Le persone autorizzate al trattamento dei dati sono responsabili della custodia e dell'utilizzo diligente e consapevole delle proprie credenziali di autenticazione che devono essere gestite attenendosi alle sotto elencate regole tecniche.
- L'autenticazione al PC e/o agli applicativi dovrà avvenire mediante utilizzo di sistemi di autenticazione a due fattori ovvero mediante autenticazione biometrica anche associati a procedure OTP, nelle more dell'attivazione di detti sistemi, idonei a garantire la sicurezza del trattamento, la password deve:

□ essere generata autonomamente dall'autorizzato al trattamento, abilitato alla consultazione delle banche dati necessarie per l'espletamento di funzioni istituzionali nell'ambito della gestione del Sistema di Videosorveglianza, all'atto del primo accesso ed essere mantenuta segreta con divieto assoluto di comunicazione a terzi o di condivisione;

□ essere di almeno 8 caratteri, ma deve essere consentita una lunghezza massima di almeno 64 caratteri con utilizzo di tutti i caratteri ASCII (RFC 20);

□ non presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti;

□ non contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;

□ non essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere) o che si riferiscano ad informazioni personali;

□ non essere memorizzata in funzioni di log-in automatico, come per esempio il completamento;

□ non essere associata a c.d. "domande di sicurezza";

□ poter essere gestita mediante la funzionalità di "incolla" in fase di inserimento per facilitare l'uso dei gestori di password (i password manager), ampiamente consigliati perché aumentano la probabilità che gli utenti scelgano password più forti;

□ poter essere inserita in chiaro, evitando l'utilizzo di punti o asterischi;

ove tecnicamente possibile, i requisiti di cui ai punti sopra indicati sono imposti da meccanismi automatici del sistema;

- la password deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- la persona autorizzata è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;
- qualora, in caso di prolungata assenza o impedimento della persona autorizzata , si verificasse la necessità di accedere ai dati ed agli strumenti elettronici per esigenze di operatività e di sicurezza del sistema, il Titolare o la persona fisica dal Titolare espressamente designata provvede ad eseguire l'accesso autonomamente utilizzando le proprie credenziali di autenticazione – in quanto configurate secondo un profilo di autorizzazione sovraordinato rispetto a quello delle persone autorizzate, propri sottordinati gerarchici – redigendo un verbale di operazioni compiute. In tal modo è garantita la piena tracciabilità dell'accesso che sarà comunque registrato mediante i file di log. Al rientro in servizio della persona autorizzata assente ovvero impedita, il Titolare o la persona fisica dal Titolare espressamente designata provvederà ad informarlo dell'accaduto consegnandogli copia del verbale di operazioni compiute;
- le credenziali di autenticazione individuali per l'accesso al profilo dell'utente, all'elaboratore ovvero alle applicazioni, non devono mai essere condivise tra più utenti (anche se Autorizzati al trattamento). Se un dipendente dovesse avere la necessità di trattare gli stessi dati o di usare le stesse procedure alle quali può accedere un collega, dovrà richiedere, al Titolare del trattamento ovvero all'Amministratore di Sistema, che gli siano assegnate le proprie credenziali di autenticazione, dotate dei privilegi necessari all'accesso ai dati o ai servizi richiesti;
- se la persona autorizzata sospetta che le proprie credenziali di autenticazione abbiano perso il requisito della segretezza (ad es. perché crede che queste siano conosciute anche da altri colleghi) è tenuto immediatamente a procedere al cambio della propria password, come espressamente previsto dalla pubblicazione NIST SP 800-63 "Digital Identity Guidelines" alla quale si rinvia integralmente.

Si precisa inoltre che, i soggetti designati come "persone autorizzate al trattamento" possono accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti ed alle funzioni istituzionali loro assegnate.

In caso di allontanamento anche temporaneo dal posto di lavoro, l'autorizzato dovrà verificare che non vi sia la possibilità da parte di terzi, anche se dipendenti dell'Ente, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato.

Nessun dato potrà essere comunicato a terzi, nell'esercizio del diritto di accesso agli atti ovvero diffuso senza la preventiva autorizzazione del Dirigente/Titolare di PO.

Il Sindaco
Cau Mauro
firmato digitalmente

COMUNE DI BARESSA ★ Prov. di Oristano ★