ORIGINALE

COMUNE DI SCICLI

Libero Consorzio Comunale di Ragusa

SETTORE VI

POLIZIA LOCALE

DETERMINAZIONE **N. 14** **DEL 09.02.2021**

REGISTRO GENERALE **N.** 167 **DEL** 10-2-2021

OGGETTO: Individuazione e nomina incaricati del trattamento dei dati personali relativi alla gestione del sistema di videosorveglianza installato nel territorio del Comune di Scicli

IL COMANDANTE

Premesso che:

- il 25 maggio 2018 è entrato in vigore il Regolamento (UE) 679/2016 (GDPR – General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

Visto l'articolo 4 del suddetto regolamento che definisce:

- Titolare del trattamento dati " l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali";
- Responsabile del trattamento: la persona fisica che tratta dati personali per conto del titolare del trattamento;
- Terzo: la persona fisica autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Considerato che occorre dar corso all'adeguamento gestionale, organizzativo, documentale e procedurale necessario per garantire la sicurezza dei dati conformemente alle disposizioni del GDPR, con particolare riferimento al sistema di videosorveglianza del Comune di Scicli;

Viste le indicazioni del garante per la protezione dei dati personali, le quali ritengono ammissibile la figura dell'incaricato del trattamento, in quanto fa riferimento alla sopradescritta definizione del "terzo";

Ritenuto, nominare quali incaricati del trattamento il personale, assegnato al VI settore – Comando di Polizia Municipale, che nell'espletamento delle proprie mansioni professionali e dei processi/procedimenti assegnati, è tenuto a trattare dati personali, sensibili e giudiziari, mediante l'impianto di videosorveglianza del Comune di Scicli;

Ritenuto altresì nominare incaricato del trattamento dati il titolare della ditta che ha fornito e realizzato l'impianto di videosorveglianza e ne effettua attualmente la manutenzione, Electrical Systems con sede in Scicli in Via Ospedale n. 12 , C.F. PCTFNC74S25I535B, Sig. Pacetto Franco;

Visto il Regolamento Comunale per la disciplina della videosorveglianza approvato con delibera di Consiglio Comunele n. 27 del 08.03.2012;

Considerato, che ai sensi del predetto regolamento che, gli impianti di videosorveglianza sono finalizzati a:

a) prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini;
b) a tutelare gli immobili di proprietà o in gestione dell' Amministrazione Comunale e a prevenire eventuali atti di vandalismo o danneggiamento del patrimonio pubblico o di disturbo della quiete pubblica;
c) al monitoraggio del traffico veicolare, identificazione degli ingorghi, compresa la rilevazione delle targhe;
d) al controllo in materia di abbandono dei rifiuti, contrastando il fenomeno del degrado urbano;
e) al controllo di determinate aree tutelando in tal modo coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un elevato gradi di sicurezza nelle zone monitorate;

f) all'attivazione quale strumento al servizio della Protezione Civile sul territorio di Scicli;
g) alla comunicazione agli utenti della strada delle vie di maggior intensità di traffico ed ogni altra notizia sulla viabilità;
h) alla rilevazione di dati anonimi per l'analisi dei flussi di traffico e per la predisposizione dei piani comunali del traffico;
i) alla vigilanza del traffico veicolare

Considerato, che ai sensi dell'art 10 del citato regolamento il dati personali devono essere raccolti e registrati per le finalità di cui all'art. 4 e conservati per un periodo non superiore a quello strettamente necessario al soddisfacimento delle finalità istituzionali dell'impianto, per le quali essi sono stati raccolti o successivamente trattati ed in ogni caso pari al periodo di tempo indicato dall'art. 10 c.4 del regolamento per la disciplina della videosorveglianza;

Visto, in materia di videosorveglianza, il provvedimento dell'08 aprile 2010, del garante per la protezione dei dati personali, che richiama le disposizioni di legge che hanno attribuito ai Sindaci e ai comuni specifiche competenze volte a garantire l'incolumità pubblica e la sicurezza urbana e precisa che:

- gli interessati al trattamento dati devono essere sempre informati che stanno per accedere in una zona videosorvegliata. L'informativa può non essere resa quando i dati personali sono trattati per il perseguimento delle finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione di reati;

- il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e , nei casi in cui sia indispensabile, a visionare le immagini (punto 3.3.2). occorre altresì distinguere coloro che sono abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (copiare, modificare lo zoom, ecc.);

- la durata di conservazione delle immagini (punto 3.4) per i Comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata della conservazione dei dati è limitata ai sette giorni successivi alla rilevazione delle immagini, fatte salve speciali esigenze ... Un eventuale allungamento dei tempi deve essere sottoposto a verifica del Garante ...;

Vista la determina Sindacale n. 02 del 29.01.2021 con cui vengono prorogati gli incarichi relativi alla titolarità dell'area delle posizioni organizzative fino al 30/11/2020;

Visti

- il vigente Regolamento comunale sull'ordinamento generale degli Uffici e dei Servizi;
- le LL.RR. nn. 48/91, 10/91, 7/92, 23/98 e 30/2000 e ss.mm.ii.;
- il D. Lgs. n. 267 del 2000;
- l'art. 48 del vigente Statuto Comunale;
- il piano triennale di prevenzione della corruzione per il triennio 2020-2022 approvato con delibera di Giunta Comunale n. 05 del 20.01.2020.

D E T E R M I N A

per le motivazioni in premessa che qui si intendono espressamente richiamate e trascritte:

1. di dare atto che il trattamento dei dati eseguito dalla Polizia Locale in relazione alla gestione del sistema di videosorveglianza installato nel territorio comunale avviene per le finalità di sicurezza urbana e per le altre finalità codificate nell'apposito regolamento comunale, indicate in premessa. Il trattamento avviene altresì secondo le indicazioni del Garante per la protezione dei dati personali (provvedimento dell'08 aprile 2010);
2. di dare atto , pertanto che il termine massimo di durata della conservazione delle immagini, come previsto al punto 3.4 del predetto provvedimento del Garante, è limitato ai sette giorni successivi, alla rilevazione delle immagini, fatte salve speciali esigenze ... Un eventuale allungamento dei tempi dovrà essere sottoposto a verifica del Garante;
3. di designare, con decorrenza immediata e fino a nuova disposizione, i sottoelencati dipendenti:

n.	DIPENDENTE
1	C.I.S. Guccione Giovanni
2	Isp. Princ. Grimaldi Fiorella
3	Isp. Princ. Mammana Antonino

assegnati al Settore VI ", incaricati del trattamento dei dati personali acquisiti dal sistema di videosprveglianza del Comune di Scicli;

4. di individuare quale soggetto " incaricato" del trattamento dati acquisiti tramite l'impianto di videosorveglianza, in relazione all'attività svolta, il Sig. Pacetto Franco, nato a Scicli il 25/11/1974, titolare e legale rappresentante dell'Impresa Electrical Systems con sede in Scicli in Via Ospedale n. 12 , C.F. PCTFNC74S25I535B, che ha realizzato l'impianto di videosorveglianza e ne cura in atto la manutenzione. Il suddetto incaricato dovrà adottare altresì le misure di sicurezza a protezione del sistema al fine di evitare accessi non autorizzati.

5. Il suddetto personale, autorizzato all'accesso al sistema di vedeosorveglianza:

- dovrà eseguire il trattamento dei dati acquisiti dal sistema di videosorveglianza unicamente per le finalità istituzionali indicate nel vigente Regolamento Comunale di videosorveglianza e nella vigente legislazione in materia, tra cui il provvedimento del garante per la protezione dei dati personali del 08 aprile 2010;
- provvederà alla gestione del sistema e dei dati acquisiti, curerà il monitoraggio della funzionalità del sistema e l'estrapolazione delle immagini;
- provvederà a segnalare alla scrivente, ai fini della successiva comunicazione agli organi competenti, la rilevazione di immagini di fatti identificativi di ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica o della tutela ambientale e del patrimonio. In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa, l'incaricato procederà alla registrazione delle stesse su supporti digitali;
- potrà consentire l'accesso alle informazioni raccolte agli Organi di Polizia e all' Autorità Giudiziaria previa richiesta motivata;
- potrà intervenire, in situazioni di necessità o su richiesta degli Organi di Polizia, sull'impianto effettuado le necessarie operazioni (es. spostare l'angolo visuale, modificare lo zoom, ecc.)
- curerà la conservazione delle eventuali immagini estrapolate o escluse dalla distruzione automatica in quanto attinenti o rilevanti per le finalità di videosorveglianza che dovranno essere salvate su apposito dispositivo;
- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per le finalità inerenti all'attività svolta;
- gli obblighi di riservatezza, alla comunicazione e alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro;

6. di dare atto che tutto il personale incaricato dovrà rispettare le seguenti specifiche misure di sicurezza per il trattamento dati di videosorveglianza:

a) divieto di comunicazione e/o diffusione delle immagini e dei dati senza la preventiva autorizzazione del responsabile del trattamento dati;

b) l'accesso alle immagini e ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente degli orari lavorativi;

c) l'accesso all'area della centrale operativa ove son installati i monitor di controllo delle immagini è assolutamente vietato al personale non autorizzato.

7. di allegare al presente provvedimento, quale parte integrante e sostanziale delle " istruzioni sul trattamento dei dati personali" (allegato A) , cui attenersi nello svolgimento delle mansioni d'ufficio assegnate;

8. di dare atto che il presente provvedimento non comporta impegno spesa;

9. E' revocato qualsiasi altro provvedimento in contrasto con la presente determinazione;

10. di disporre che la presente sarà trasmessa in orginale al segreteria generale ed in copia ai soggetti incaricati del trattamento dati e per opportuna conoscenza al Sindaco, all' Assessore al Personale, al Segretario Comunale n.q. di Responsabile Prevenzione della Corruzione .

11. di disporre la pubblicazione del presente provvedimento all'albo pretorio on line del Comune di Scicli per quindici giorni consecutivi.

COMUNE DI SCICLI
CORPO P.M.

Il Comandante
Dott.ssa Maria Rosa Portelli

COMUNE DI SCICLI

Libero Consorzio Comunale di Ragusa
SETTORE VI
Comandi di Polizia Locale

ISTRUZIONI SUL TRATTAMENTO DEI DATI PERSONALI

DEFINIZIONI

" **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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

" **Categorie particolari di dati personali":** i dati personali idonei a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati genetici e biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

" **Dati giudiziari**": i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

"**Trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

" **Violazione dei dati personali**":la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

ISTRUZIONI

Nella gestione dei processi/procedimenti dell'ufficio a cui ciascun incaricato è preposto e, più in generale, nello svolgimento dell'attività lavorativa presso il Settore IV, ciascun incaricato del trattamento dei dati personali ha l'obbligo di attenersi scrupolosamente alle istruzioni di seguito fornite:

- effettuare trattamenti dei dati personali nel rispetto delle norme e misure di sicurezza previste dal Regolamento UE 679/2016;
- trattare i dati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccogliere i dati per finalità determinate, esplicite e legittime e successivamente trattarli in modo che non sia incompatibile con tali finalità;
- utilizzare informative e consensi (se necessari) per la privacy;
- raccogliere i dati solo per le specifiche finalità del trattamento assegnato;
- conservare i dati per un periodo non superiore a quello necessario al raggiungimento delle finalità del trattamento ;

- porre in essere tutte le attività e condotte dirette a garantire un'adeguata sicurezza dei dati, compresa la protezione da trattamenti non autorizzati o illeciti,e ad evitare la perdita, la distruzione o il danno accidentale;
- riferire al responsabile del trattamento ogni violazione di dati personali di cui viene a conoscenza senza ritardo;
- riferire al responsabile del trattamento ogni trattamento di dati personali nuovo rispetto a quelli già noti nell'ufficio di propria competenza, al fine di consentirne la valutazione del rischio;

MISURE DI SICUREZZA

<u>In caso di trattamenti senza l'ausilio di strumenti elettronici è necessario:</u>

- controllare e custodire gli atti e i documenti contenenti dati personali durante la sessione di lavoro;
- custodire con la cura necessaria, al fine di garantire la massima riservatezza, i documenti contenenti i dati personali in un armadio o in un cassetto chiusi a chiave o comunque non accessibili alle persone non autorizzate;
- non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali;
- custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicando tempestivamente lo smarrimento o il furto al proprio referente;
- in caso di allontanamento, anche temporaneo, dal posto di lavoro, verificare che non vi sia la possibilità da parte di terzi di accedere ai dati personali per i quali era in corso una qualunque operazione di trattamento;
- prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;

<u>In caso di trattamenti effettuati con l'ausilio di strumenti elettronici è necessario:</u>

- utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro;
- custodire le proprie credenziali in un luogo sicuro ed avvisare tempestivamente il titolare del trattamento dati in caso di smarrimento o sottrazione;
- mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o farla utilizzare a terzi;
- conservare eventuali supporti magnetici rimovibili utillizzati nel trattamento (CD, dischetti, pen drive, USB) con i medesimi accorgimenti previsti per i supporti cartacei;
- proteggere i computer in caso di assenza, anche temporanea, dalla postazione di lavoro, tramite la sospensione o il blocco della sessione di lavoro.