COMUNE DI VEGLIE

(Provincia di Lecce)

COPIA

DETERMINAZIONE DEL RESPONSABILE

DEL

5. SETTORE PIANIFICAZIONE DEL TERRITORIO E PATRIMONIO

SERVIZIO

Numero 56 Settoriale del 13/05/2024

Numero 315 Reg. Generale del 13/05/2024

OGGETTO: NOMINA DELLE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI, AI SENSI DEGLI ARTT. 4 E 29 DEL REGOLAMENTO EUROPEO 679/2016 (GDPR).

L'anno 2024 il giorno 13 del mese di MAGGIO, nel proprio Ufficio presso la Sede Municipale, il sottoscritto **Ing. Mauro MANCA,** Responsabile del 5. SETTORE PIANIFICAZIONE DEL TERRITORIO E PATRIMONIO - Servizio :

Visti:
· il D.Lgs 18.08.2000 n. 267;
· il vigente Statuto comunale;
· il vigente Regolamento per l'Organizzazione degli Uffici e dei Servizi;
· il vigente Regolamento di Contabilità;
· il decreto sindacale di attribuzione della responsabilità del Settore;
· l'adempimento ex art. 48 bis del DPR 602/73 introdotto dal L. 286/2006;

Dato atto, ai sensi e per gli effetti del disposto di cui agli artt.49 e 147 – bis del D.Lgs. n. 267/2000 e di quanto previsto dal vigente regolamento dei controlli interni, che nella fase preventiva di formazione del presente atto si è eseguito idoneo controllo di regolarità amministrativa e che, con la firma apposta in calce all'originale del presente atto, se ne attesta, anche, la legittimità, la regolarità e la correttezza dell'azione amministrativa;

Premesso:

- che, nell'ambito dei poteri di organizzazione delle attività rimesse alla loro responsabilità, i Titolari del ruolo di "Elevata Qualificazione" (già Posizione Organizzativa) possono individuare articolazioni di dettaglio nell'esercizio della loro responsabilità;
- con Decreto del Sindaco n. 01 del 07/02/2024 lo scrivente è stato designato quale "Delegato al trattamento dei dati personali" ai fini dell'espletamento delle attività relative all'adeguamento dell'Ente alla normativa riguardante la protezione dei dati personali.

Rilevato che, ai fini dell'osservanza delle disposizioni contenute nel Regolamento UE 679/2016 - GDPR, vanno anzitutto individuati gli attori, i ruoli e le responsabilità del sistema organizzativo preordinato a garantire la protezione dei dati personali.

Richiamati gli articoli 4 e 29 del Regolamento Europeo 679/2016, che in particolare dispongono:

- Art. 4 (definizioni) "[…] ... «terzo»: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile*;
- Art. 29 (Trattamento sotto l'autorità del Titolare del trattamento […]) […] ... *chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento* … […]".

Constatato che:

- - è necessario attuare la migliore qualità conseguibile nel trattamento dei dati personali, e ciò è possibile attuando in piena autonomia la gestione dei compiti del proprio Settore;
- - risulta necessario configurare il proprio Settore, secondo criteri di efficienza e efficacia, delegando compiti operativi a personale che possieda abilità e formazione opportune per svolgere le mansioni a esso delegate;

- - a seguito di apposita attività conoscitiva e valutativa, è risultato che le dipendenti assegnate al Settore Pianificazione del Territorio e Patrimonio, offrono garanzie sufficienti circa le proprie qualità professionali e personali, in particolare esperienza, capacità e affidabilità, nonché della capacità di assolvere i compiti con scrupolosità e diligenza.

Preso atto che attualmente sono assegnati al Settore Settore Pianificazione del Territorio e Patrimonio, i dipendenti come di seguito identificati in ordine alfabetico:

- Bianco Giuseppe;
- Mazzotta Loredana
- Romano Paolo.

DETERMINA

1. Di individuare i dipendenti assegnati al Settore Settore Pianificazione del Territorio e Patrimonio, come identificate in narrativa, quali "Persone autorizzate al trattamento *ex* artt. 4 e 29 del Regolamento Europeo 679/2016, per i trattamenti necessari per l'espletamento delle mansioni ricoperte all'interno dell'Ente.
2. Di precisare che i compiti e le funzioni a tal fine assegnate sono analiticamente elencate nell'allegato al presente provvedimento, costituendone parte integrante e sostanziale, con facoltà di successiva integrazione e/o modificazione, dando atto che l'attribuzione di compiti e funzioni inerenti il trattamento dei dati personali non implica l'attribuzione di compiti e funzioni ulteriori rispetto a quelli propri della qualifica rivestita ma conferisce soltanto il potere/dovere di svolgere i compiti le funzioni attribuite.
3. Di dare atto, altresì, che:

- tale ruolo ha validità per l'intera durata del rapporto / incarico di dipendenza;
- tale ruolo viene a cessare al modificarsi del rapporto / incarico di dipendenza;
- tale ruolo viene a cessare in caso di revoca espressa;
- tale ruolo non consente l'attribuzione ad altri soggetti di poteri e compiti qui previsti;
- al cessare di tale ruolo, rimane inibito e comunque non autorizzato ogni ulteriore esercizio dei compiti e delle funzioni trattamento dei dati personali oggetto del presente provvedimento, salvo che ciò sia imposto o consentito da una norma di Legge o da un provvedimento dell'autorità ovvero sia necessario ad esercitare o difendere un diritto.

4. Di dare atto che il presente provvedimento integra gli atti a suo tempo adottati.
5. Di stabilire che il presente atto e la trasmissione del presente atto e l'annesso Allegato venga trasmesso ai destinatari sopra "Autorizzati" e comunicato al Responsabile della Protezione dei Dati – DPO.
6. Di precisare infine che, al verificarsi di eventuali modifiche alla struttura organizzativa del Settore, lo stesso qui presente provvedimento e l'annesso Allegato vengano trasmessi alla/e nuove risorse umane

eventualmente assegnatevi, e comunicati al DPO.

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI

SOTTO IL PROFILO DEL TRATTAMENTO DI DATI PERSONALI:

Nello svolgere le proprie funzioni, che comportino un trattamento di dati personali, deve attenersi alle seguenti ulteriori istruzioni:

- in attuazione del principio di «liceità, correttezza e trasparenza»,
    - le operazioni di raccolta, registrazione, elaborazione di dati ed in generale, le operazioni di trattamento tutte, avvengono agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati presenti nella struttura di propria competenza, nell'osservanza delle tecniche e metodologie in atto;
    - autorizzazione a comunicare od eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente, per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal Titolare del trattamento;
- in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui è preposto;
- in attuazione del principio di «limitazione della finalità» il trattamento deve essere conforme alle finalità istituzionali del Titolare e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, ed obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;
- in attuazione del principio di «limitazione della conservazione»
    - conservare i dati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati e obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nella struttura di competenza, dati personali non necessari o divenuti ormai superflui. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti i dati di cui agli articoli 9 e 10 del GDPR vengano conservati in contenitori/armadi muniti di serratura od in ambienti ad accesso selezionato e vigilato, fatte salve le norme in materia di archiviazione amministrativa;
- in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente ed integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal Titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. In particolare:
    - riporre in archivio, al termine del periodo di trattamento, i supporti ed i documenti, ancorché non definitivi, contenenti i dati personali;
    - non fornire dati personali per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
    - evitare di inviare, per fax, documenti in chiaro contenenti dati personali: si

suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'Interessato (ad esempio, contrassegnando i documenti semplicemente con un codice). In alternativa, si suggerisce di avvisare preventivamente il destinatario della comunicazione fax in modo che possa curarne la diretta ricezione;

- In attuazione del principio di «trasparenza»:
  - accertarsi dell'identità dell'Interessato, prima di fornire informazioni circa i dati personali od il trattamento effettuato;
  - fornire all'Interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 ed all'articolo 34 del GDPR, relative al trattamento utilizzando apposita modulistica. Se richiesto dall'Interessato, le informazioni medesime possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'Interessato;
  - conservare, nel rispetto del principio di Accountability, tutte le versioni delle informative in uno specifico archivio interno cartaceo e telematico e tenere traccia di tutte le modifiche al testo (connesse alle modifiche organizzative, tecniche e normative) al fine di consentire al Titolare una maggiore tutela in sede amministrativa e/o giudiziaria nel caso di reclami o procedimenti giudiziari per risarcimento di danni conseguenti a trattamenti illeciti di dati;
  - agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del GDPR;
- nel caso di presenza di utenti, ospiti o personale di servizio, all'interno dell'Ufficio, sarà necessario:
  - fare attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;
  - evitare di allontanarsi dalla scrivania o riporre i documenti ed attivare il salvaschermo del PC;

Le stesse istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici, contenuti in archivi/banche dati o destinati a figurarvi.

In particolare, per tali trattamenti la persona fisica Autorizzata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

A) Strumenti elettronici in generale

- ✓ i personal computer fissi e portatili ed i programmi per elaboratore su di essi installati sono uno strumento di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della normativa sulla protezione dei dati personali: vanno, pertanto, utilizzati e conservati, insieme ai relativi documenti esplicativi, con diligenza e cura, attenendosi alle prescrizioni fornite dal Titolare e nel rispetto delle indicazioni da questo fornite;
- ✓ in generale tutti i dispositivi elettronici sono forniti per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare pertanto eccezionale e limitato a comunicazioni occasionali e di breve durata, ad esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali;
- ✓ le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dagli addetti informatici incaricati sulla base di criteri e profili decisi dal Titolare, in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti

stabilita dall'Amministrazione stessa. Il dipendente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione.

✓ assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione o distruzione dei supporti di memorizzazione dei dati;

✓ rivolgersi tempestivamente, per difficoltà o questione inerente la sicurezza, al competente superiore;

✓ per finalità di assistenza, manutenzione ed aggiornamento e previo consenso esplicito del dipendente stesso, l'Amministratore di Sistema o soggetti appositamente incaricati allo svolgimento di tale attività potranno accedere da remoto al personal computer del dipendente attraverso un apposito programma "software";

✓ il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici di cui fa uso, tra cui ad esempio fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari, pen-drive e supporti di memoria;

✓ al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'Ente per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

L'Ente ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati.

B) Predisposizione di atti e documenti da pubblicare sul sito web istituzionale

✓ adottare opportuni accorgimenti prima di procedere alla pubblicazione sul sito internet istituzionale (in sostituzione del responsabile della pubblicazione dell'Ente) tra cui:

- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;

- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;

- sottrarre all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) i dati sensibili e giudiziari.

Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

C) Password e username (credenziali di autenticazione informatica)

✓ per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui ed astenendosi dall'accedere a servizi telematici non consentiti. Le credenziali di autenticazione informatica sono individuali. Non possono essere condivise;

✓ è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;

✓ i codici identificativi, le password e le smart card saranno disattivate nel caso in

cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa. In tali casi il dipendente è tenuto a restituirle agli uffici a ciò preposti.

✓ la password che la persona fisica designata e autorizzata al trattamento imposta, con il supposto e l'assistenza, in caso di difficoltà, dell'Amministratore di Sistema (se esistente) o dell'Ufficio competente. La stessa:

- deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri (almeno 8 caratteri);
- non deve essere riconducibile alla persona;
- deve essere cambiata almeno ogni 3/6 mesi;
- non deve essere rivelata o fatta digitare al personale di assistenza tecnica;
- non deve essere rivelata o comunicata al telefono, via fax od altra modalità elettronica;

D) Assenza od impossibilità temporanea o protratta nel tempo

✓ nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività del Titolare sia necessario accedere ad informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare a un altro dipendente a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.

✓ in caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'ufficio sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, il Responsabile di Settore a cui è assegnato il dipendente può richiedere con apposita e motivata richiesta all'Amministratore del Sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il Responsabile di Settore deve informare il dipendente dell'avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

E) Log-out

✓ In caso di allontanamento anche temporaneo dalla postazione di lavoro (personal computer fisso o portatile), il dipendente non deve lasciare il sistema operativo aperto con la propria password e/o smart card inserita. Al fine di evitare che persone estranee effettuino accessi non consentiti, il dipendente deve attivare il salvaschermo con password o deve bloccare il computer e togliere la smart card dall'apposito alloggiamento.

F) Utilizzo della rete internet e relativi servizi - Cloud storage

✓ non è consentito navigare in siti web non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;

✓ è da evitare la registrazione a servizi on-line, a titolo o per interesse personale;

✓ non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi

comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto;

✓ non è permessa la partecipazione, per motivi non professionali, a servizi di forum, l'utilizzo di chat-line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);

✓ il dipendente si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).

G) Posta elettronica

✓ la casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa;

✓ l'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'Ente. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale;

✓ si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica assegnati per le comunicazioni personali;

✓ al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali dell'Ente, eventualmente affiancandoli a quelli individuali;

✓ le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.

✓ non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o che possano essere in qualunque modo fonte di responsabilità dell'Ente;

✓ il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'Ente. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile;

✓ la posta elettronica diretta all'esterno della rete dell'Ente può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti contenenti dati personali di cui agli articoli 9 e 10 del GDPR;

✓ non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale dell'Ente per la partecipazione a dibattiti, Forum o mail-list, salvo diversa ed esplicita autorizzazione;

✓ qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l'Amministratore di sistema o il Responsabile competente.

H) Software, applicazioni e servizi esterni

✓ onde evitare pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dall'Amministratore di sistema o figura analoga ovvero dal Responsabile di riferimento.

✓ non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

✓ non è consentito modificare le configurazioni impostate sul proprio PC;

✓ non è consentito configurare gli strumenti per la gestione della posta elettronica per la gestione di account privati. Non è inoltre consentito utilizzare detti strumenti per la ricezione, visualizzazione ed invio di messaggi a titolo personale;

✓ il Titolare si riserva la facoltà di procedere alla rimozione di ogni file od applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti od installati in violazione delle presenti istruzioni;

✓ tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi, (salvo quando questo sia richiesto dall'amministratore di sistema per compiere attività di manutenzione o aggiornamento).

I) Reti di comunicazione

✓ nel caso di trattamento di dati personali effettuato mediante elaboratori non accessibili da altri elaboratori (cioè mediante computer stand alone) è necessario utilizzare la parola chiave (password) fornita per l'accesso al singolo PC;

✓ nel caso di trattamento di dati personali effettuato mediante elaboratori accessibili da altri elaboratori, solo in rete locale, o mediante una rete di telecomunicazioni disponibili al pubblico, è necessario: utilizzare la parola chiave (password) fornita per l'accesso ai dati, oltre a servirsi del codice identificativo personale per l'utilizzazione dell'elaboratore;

✓ le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque "file" che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;

✓ al fine di garantire la disponibilità dei documenti di lavoro assicurandone il backup periodico, si dovrà procedere al loro salvataggio nell'apposita area di rete individuale o di gruppo a ciò dedicata e disponibile sui sistemi server del Titolare;

✓ non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare.

✓ non condividere file, cartelle, hard-disk o porzioni di questi del proprio

computer, per accedere a servizi non autorizzati di peer to peer al fine condividere materiale elettronico tutelato dalle normative sul diritto d'autore (software, file audio, film, etc.).

J) Utilizzo dei mezzi di informazione e dei social media

✓ nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza;

✓ in ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'Ente;

✓ al fine di garantirne i necessari profili di riservatezza, le comunicazioni afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

K) Supporti esterni di memorizzazione

La persona fisica designata e autorizzata al trattamento, ha l'obbligo di:

- utilizzare i supporti di memorizzazione solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- proteggere i dati personali archiviati su supporti esterni con le stesse misure di sicurezza previste per i supporti cartacei;
- verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;
- evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
- copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento; copie di dati contemplati dagli articoli 9 e 10 del GDPR devono essere espressamente autorizzate. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione.
- procedere alla cancellazione dei supporti esterni contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- verificare l'assenza di virus nei supporti utilizzati;

Il presente documento approvato viene sottoscritto.

IL RESPONSABILE DEL SETTORE
f.to Ing. Mauro MANCA

CERTIFICATO DI PUBBLICAZIONE

Reg. N. 698

Certifico che la presente determinazione viene pubblicata dal 15/05/2024 al 30/05/2024 all'Albo Pretorio del Comune.

Veglie, lì

IL SEGRETARIO GENERALE
f.to Dott. Pierluigi CANNAZZA

Documento firmato digitalmente ai sensi del TU n. 445/00, dell'art. 20 del D.lgs. 82/2005 e norme collegate. Tale documento informatico è memorizzato digitalmente sulla banca dati dell'Ente.