



COMUNE DI COLLI VERDI

Provincia di Pavia

Località Pometo - Piazza Municipio - Frazione Ruino, n. 1 - CAP 27061

C.F./P.I. 02738210182

tel. 0385955898 – fax 0385955897

comune.colliverdi@legalpec.it

info@comune.colliverdi.pv.it

DECRETO SINDACALE N. 4

OGGETTO: MISURE FINALIZZATE A DARE ATTUAZIONE ALLE DISPOSIZIONI DEL REGOLAMENTO (UE) N. 2016/679 – ATTO DI DESIGNAZIONE DEI RESPONSABILI IN RELAZIONE AL TRATTAMENTO DEI DATI PERSONALI.

L'anno duemilaventuno addì ventuno del mese di settembre il Sindaco, in merito all'oggetto sopra indicato adotta il seguente decreto:

IL SINDACO

Visto 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 (di seguito solo GDPR);

Rilevato che, ai fini dell'osservanza delle disposizioni contenute nel GDPR, vanno innanzitutto individuati gli attori, i ruoli e le responsabilità del sistema organizzativo preordinato a garantire la protezione dei dati personali;

Dato atto che, in considerazione dell'entrata in vigore della nuova normativa del GDPR e della modificata definizione di Responsabile del trattamento, si rende necessario procedere all'adozione degli atti di nomina degli autorizzati, al fine di attribuire ai medesimi, in qualità di soggetti appositamente designati, specifici funzioni e compiti connessi al trattamento dei dati personali;

Dato atto che a seguito della pubblicazione del Decreto Legislativo 10 agosto 2018 n. 101 contenente *“Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679”*, è stato introdotto all'interno del Decreto Legislativo 30 giugno 2003 n. 196 (Codice della privacy) l'articolo 2-quaterdecies rubricato *“(Attribuzione di funzioni e compiti a soggetti designati)”* il quale così dispone: *“1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. 2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta”*.

Considerato che, conformemente alle disposizioni del GDPR, e della normativa interna di adeguamento, il Titolare ed il Responsabile del trattamento possono quindi designare, sotto la propria responsabilità, ed all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati;

Dato atto che si rende necessario procedere alla designazione delle persone fisiche aventi specifici compiti e funzioni connessi al trattamento dei dati personali, ed alla delega dell'esercizio e dello svolgimento di tali specifici compiti e funzioni alle persone fisiche designate;

Ritenuto di attribuire ai designati/ autorizzati gli specifici compiti e funzioni spettanti al Titolare ed analiticamente elencati in calce al presente atto, ferma restando l'imputazione della responsabilità conseguente al trattamento in capo al Titolare medesimo;

Rilevato, al riguardo, che ai Responsabili di Servizio spettano l'adozione degli atti e provvedimenti amministrativi, compresi tutti gli atti che impegnano l'amministrazione verso l'esterno, la gestione finanziaria, tecnica ed amministrativa mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo, nonché, in via esclusiva, dell'attività amministrativa, della gestione e dei risultati della struttura organizzativa a cui sono preposti;

Considerata l'esigua struttura organizzativa e l'organigramma funzionale degli Uffici e dei servizi di questo Ente che conta solamente n. 7 dipendenti/incaricati preposti all'attività amministrativa:

AREA	SERVIZI	PERSONALE ASSEGNATO
AREA 1 TRIBUTI - AMMINISTRATIVO - DEMOGRAFICO ED ELETTORALE - INFORMATIVO - SPORT E TEMPO LIBERO	<ol style="list-style-type: none"> 1. Servizi demografici 2. Servizi generali, segreteria, rapporti con associazioni 3. Servizi informatici 4. Tributi 5. Sport e Tempo Libero 	FERRI BARBARA LOLLA ILARIA MARZI ROBERTO VERCESI CAMILLA
AREA 2 - SERVIZIO ECONOMICO E FINANZIARIO, ISTRUZIONE, CULTURA E SERVIZI ALLA PERSONA	<ol style="list-style-type: none"> 1. Servizi finanziari e ragioneria 2. Servizio commercio 3. Servizio economato 4. Servizi istruzione, turismo e cultura 5. Servizi alla Persona 	DEGLI ANTONI STEFANO
AREA 3 PATRIMONIO, LAVORI PUBBLICI, PROTEZIONE CIVILE URBANISTICA	<ol style="list-style-type: none"> 1. Servizi manutentivi patrimonio, demanio, viabilità, ambiente 2. Servizi di programmazione lavori pubblici, progettazione nuove opere e affidamento lavori, CUC 3. Servizio protezione civile 4. Ufficio adempimenti decreto 81/2008 in materia di sicurezza sui luoghi di lavoro 5. Urbanistica ed edilizia privata 	MONTECUCCO PAOLA MARIA
AREA 4 POLIZIA LOCALE - POLIZIA RURALE - POLIZIA COMMERCIALE/ SUAP - POLIZIA AMBIENTALE - POLIZIA EDILIZIA - GESTIONE VERBALI, NOTIFICHE, ACCERTAMENTI - SUPPORTO ALL'UFFICIO ANAGRAFE, STATO CIVILE E TRIBUTI	<ol style="list-style-type: none"> 1. Sportello attività produttive 2. Servizi tecnici inerenti i cimiteri (operazioni di tumulazione, estumulazione, ecc. gestione luci votive) 3. Edilizia 4. Agricoltura e forestazione 5. Servizio per il governo del territorio 	BANDANERA GIUSEPPE BENITO

Ritenuto di designare, quali autorizzati al trattamento dei dati personali, i seguenti dipendenti che prestano servizio presso l'Ente:

BANDANERA GIUSEPPE BENITO
DEGLI ANTONI STEFANO
FERRI BARBARA
LOLLA ILARIA
MARZI ROBERTO
MONTECUCCO PAOLA MARIA
VERCESI CAMILLA

DECRETA

1. **DI DESIGNARE** quali autorizzati al trattamento ai sensi dell'art. 4 del GDPR, con decorrenza dalla data di ricezione del presente provvedimento, il personale sopra indicato che opera sotto la diretta autorità del Titolare, con compiti e funzioni connessi al trattamento di dati personali, e relativi ai trattamenti rientranti nella struttura organizzativa di competenza, elencati nel Registro dei trattamenti, dando atto che i compiti e funzioni attribuite devono essere svolti:
 - presso la sede del Titolare e le sue articolazioni territoriali;
 - nell'ambito e conformemente alle istruzioni contenute nel presente atto di designazione;
2. **DI ATTRIBUIRE**, con decorrenza dalla data di ricezione del presente provvedimento, al medesimo personale i compiti e le funzioni analiticamente elencate in allegato al presente decreto, 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 dal Responsabile;
3. **DI DARE ATTO**, altresì, che:
 - tale ruolo ha validità per l'intera durata del rapporto di lavoro;
 - tale ruolo viene a cessare in caso di revoca espressa;
 - 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 gli specifici compiti attribuiti vanno svolti nell'ambito delle funzioni assegnate connesse al trattamento dei dati personali;
5. **DI DISPORRE** la pubblicazione del presente provvedimento all'albo pretorio on line e nella sezione Amministrazione Trasparente;
6. **DI DISPORRE** la comunicazione personale, con rilascio di apposita notifica del presente atto.

IL SINDACO

Sergio Lodigiani



SOTTO IL PROFILO DEL TRATTAMENTO DI DATI PERSONALI L'AUTORIZZATO DEVE ATTENERSI ALLE SEGUENTI 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 l'Autorizzato è preposto;
- in attuazione del principio di «limitazione della finalità» il trattamento dev'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»
 - evitare, ove possibile, di creare banche dati nuove;
 - 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 la perdita, la distruzione o il 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 la modulistica all'uopo predisposta dal Titolare. 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 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 i trattamenti dei dati personali la persona fisica responsabile o autorizzata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

- **Strumenti elettronici in generale**

1. 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;
2. in generale tutti i dispositivi elettronici sono forniti al dipendente 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;
3. 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 da parte del Responsabile di P.O. competenti;
4. assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione o distruzione dei supporti di memorizzazione dei dati;
5. 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;
6. 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.

– **Password e username (credenziali di autenticazione informatica)**

1. 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 con altri incaricati del trattamento;
2. è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;
3. i codici identificativi, le password e le smart card dei dipendenti saranno disattivati 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 restituire la propria smart card agli uffici a ciò preposti;
4. la password che la persona fisica designata e delegata al trattamento imposta, con il supporto e l'assistenza, in caso di difficoltà, dell'amministratore di sistema:
 - deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri;
 - non deve essere riconducibile alla persona del designato;
 - deve essere cambiata almeno ogni 3 mesi dal designato medesimo;
 - non dev'essere rivelata o fatta digitare al personale di assistenza tecnica;
 - non dev'essere rivelata o comunicata al telefono, via fax od altra modalità elettronica. Nessuno è autorizzato a chiederla.

– **Assenza od impossibilità temporanea o protratta nel tempo**

1. 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 al responsabile dell'area in cui lavora 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;
2. 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 Dirigente / Responsabile di P.O. 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 Dirigente / Responsabile di P.O. deve informare il dipendente dell'avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

– **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 (utilizzando i tasti CTRL+ALT+CANC) e togliere la smart card dall'apposito alloggiamento.

– **Utilizzo della rete internet e relativi servizi - Cloud storage**

1. 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;

2. è da evitare la registrazione a servizi online, a titolo o di interesse personale;
3. 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 dal Dirigente / Responsabile di P.O. e con il rispetto delle normali procedure di acquisto;
4. 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);
5. la persona fisica responsabile o autorizzata al trattamento, 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.).

Posta elettronica

1. la casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa;
2. si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica assegnati dal Titolare per le comunicazioni personali;
3. 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;
4. le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.
5. 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;
6. 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;
7. 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;
8. qualora si verificano anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l'Amministratore di sistema o il Dirigente / Responsabile di P.O.

Softwares, applicazioni e servizi esterni

1. 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;
2. non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
3. non è consentito modificare le configurazioni impostate sul proprio PC;
4. 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;
5. 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;
6. 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 dai dipendenti, (salvo quando questo sia richiesto dall'amministratore di sistema per compiere attività di manutenzione o aggiornamento).

– **Reti di comunicazione**

1. 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;
2. (password) fornita per l'accesso al singolo PC;
3. 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;
4. 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;
5. al fine di garantire la disponibilità dei documenti di lavoro assicurandone il backup periodico, il dipendente dovrà procedere al loro salvataggio nell'apposita area di rete individuale o di gruppo a ciò dedicata e disponibile sui sistemi server del Titolare;
6. è proibito tentare di acquisire i privilegi di Amministratore di sistema;
7. non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare;
8. 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.).

– **Supporti esterni di memorizzazione**

La persona fisica responsabile o autorizzata al trattamento, ha l'obbligo di:

1. 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;
2. proteggere i dati personali archiviati su supporti esterni con le stesse misure di sicurezza previste per i supporti cartacei;
3. 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;
4. evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
5. 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 dal Dirigente / Responsabile di P.O. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
6. evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del Titolare o del-Dirigente / Responsabile di P.O.;
7. procedere alla cancellazione dei supporti esterni contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
8. verificare l'assenza di virus nei supporti utilizzati.