COMUNE DI
CASSANO SPINOLA
Provincia di Alessandria

DETERMINAZIONE
AREA FINANZIARIA

N. 21 DEL 26 NOVEMBRE 2019

REGOLAMENTO (UE) N. 2016/679 - DESIGNAZIONE DIPENDENTE INCARICATO AL TRATTAMENTO DEI DATI PERSONALI CONTENUTI NELLE BANCHE DATI E NEI PROCEDIMENTI INERENTI LE MATERIE RICADENTI NELL'AREA FINANZIARIA

L'anno duemiladiciannove il giorno ventisei del mese di novembre

IL RESPONSABILE DELL'AREA FINANZIARIA

Adotta la seguente determinazione

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, semplicemente, 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:
- Il GDPR non prevede espressamente la figura degli "incaricati" e, tuttavia, tale figura può essere implicitamente desunta dall'articolo 29, rubricato "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento", il quale stabilisce che "*il responsabile del trattamento, o 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, salvo che lo richieda il diritto dell'Unione o degli Stati membri*";

- 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 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;

RITENUTO che le modalità più opportune siano costituite dalla delega di compiti e funzioni alle persone fisiche designate;

ATTESO che il Comune di Cassano Spinola è il Titolare del trattamento dei dati personali e che il Sindaco rappresenta il Comune quale Titolare del Trattamento dei dati e ne svolge le relative funzioni;

RICHIAMATI:
- la deliberazione della Giunta comunale n. 60 del 23.10.2019 di approvazione del Piano di Protezione e il modello contenente le disposizioni a carattere organizzativo necessarie ed opportune a consentire la corretta applicazione della normativa, comunitaria e nazionale, in tema di protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- il decreto sindacale n. 8 del 13.11.2019, con il quale il Titolare del trattamento ha designato i Responsabili di Posizioni Organizzative e attribuito al sottoscritto Responsabile di P.O. specifici compiti e funzioni connesse al trattamento dei dati personali inerenti i servizi e le funzioni ricadenti nell'Area Amministrativa di propria competenza di cui all'allegato Funzionigramma, **allegato "1"** al presente provvedimento;

DATO ATTO che, nel suddetto decreto sindacale, sono espressamente ricompresi anche il compito e la funzione di identificare e designare, per iscritto, le persone fisiche della struttura organizzativa medesima che operano sotto la diretta autorità del Titolare, e di attribuire alle persone medesime specifici compiti inerenti al trattamento dei dati inclusa l'autorizzazione al trattamento, impartendo a tale fine analitiche istruzioni, e controllando costantemente che le persone fisiche designate e delegate al trattamento dei dati effettuino le operazioni di trattamento:

- in attuazione del principio di «liceità, correttezza e trasparenza»;
- in attuazione del principio di «minimizzazione dei dati»;
- in attuazione del principio di «limitazione della finalità»;
- in attuazione del principio di «esattezza»;
- in attuazione del principio di «limitazione della conservazione»;
- in attuazione del principio di «integrità e riservatezza»;
- in attuazione del principio di «liceità, correttezza e trasparenza».

Dato atto che alla presente struttura organizzativa: Area Finanziaria è assegnato, per il 50%, il dipendente sottoelencato:

NOME E COGNOME
Renzo Carlo REPETTO – Istruttore Direttivo

RILEVATO che il dipendente sopra menzionato:

- gestisce, per quanto rientra nelle proprie funzioni, i processi/procedimenti inerenti le materie ricadenti nell'area di propria competenza;

- effettua, in forza di atto di nomina ad incaricato, in atti, il trattamento dei dati personali, anche rientranti nelle fattispecie di cui agli articoli 9 e 10 del GDPR di tutti i processi/procedimenti e di tutti i soggetti con i quali il Titolare si relaziona nell'ambito della sua attività istituzionale connessa a tutti i processi/procedimenti dell'Ufficio;

DETERMINA

1. DI DESIGNARE, con decorrenza dalla data di ricezione del presente provvedimento, il Signore di seguito indicato, che opera sotto la diretta autorità del Titolare, quale persona fisica a cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali, relativi ai trattamenti rientranti nella struttura organizzativa di competenza:

NOME E COGNOME
Renzo Carlo REPETTO (per il 50% Area Finanziaria) – Istruttore Direttivo

2. DI DARE ATTO che:
- i compiti e funzioni attribuite, con decorrenza dalla data di ricezione del presente provvedimento, con facoltà di successiva integrazione e/o modificazione, non implicano 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 Titolare;
- detti 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;

TRATTAMENTI **rientranti nella struttura organizzativa di competenza**
L'esatta individuazione delle attività e delle finalità di trattamento, delle categorie di dati personali e di interessati, delle categorie di destinatari, dei termini ultimi previsti per la cancellazione delle diverse categorie di dati e delle misure di sicurezza tecniche ed organizzative, con specifico riferimento al destinatario del presente atto ed all'Ufficio di pertinenza, è possibile consultando il Registro istituito dal Titolare ai sensi dell'articolo 30 del GDPR.

3. DI DELEGARE, con decorrenza dalla data di ricezione del presente provvedimento, ai predetti dipendenti, che operano sotto la diretta autorità del Titolare, il compito di trattare i dati personali inerenti i servizi e le funzioni attribuite, ricadenti nell'Area, a cui sono assegnati, conferendo formale potere e autorizzazione di compiere, secondo le specifiche istruzioni e prescrizioni di cui all'allegato "2", tutte le operazioni di trattamento di dati personali;

4. DI DARE ATTO che la presente designazione e delega:
- costituisce formale autorizzazione a trattare dati personali conformemente al GDPR, alla normativa interna di adeguamento, alle Linee guida delle Autorità di controllo, alle specifiche istruzioni sulle modalità a cui attenersi nel trattamento di seguito indicate e, infine, alle eventuali indicazioni del RPD/DPO;
- non consente l'attribuzione ad altri soggetti di poteri e compiti qui previsti;
- ha validità per l'intera durata del rapporto di lavoro;

- viene a cessare al modificarsi del rapporto di lavoro o con esplicita revoca, con espresso avvertimento che, al suo cessare, rimane inibito e comunque non autorizzato ogni ulteriore 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.

5. DI COMUNICARE il presente atto al predetto personale, con rilascio di apposita dichiarazione di ricevimento dello stesso.

IL FUNZIONARIO RESPONSABILE DI AREA
(Rag. Andrea Campi)

CERTIFICATO DI PUBBLICAZIONE

Copia della presente determina viene pubblicata mediante affissione all'Albo Pretorio on line nel sito web istituzionale di questo Comune in data odierna per rimanervi quindici giorni consecutivi.

Li, 3 DICEMBRE 2019

IL MESSO COMUNALE

Allegato ”1”

FUNZIONIGRAMMA
AREA FINANZIARIA
Responsabile: Rag. Andrea Campi
UNITA’ OPERATIVE N. 1 *(assegnato per il 50%)*   • *Renzo Carlo Repetto – Istruttore Direttivo – Cat. D1*

SERVIZI E FUNZIONI COMPRESI NELL’AREA FINANZIARIA
- Contabilità e Bilancio e adempimenti fiscali
- Tributi, imposte e canoni
- Servizio Economato (*servizio cassa per minute spese d'ufficio secondo la disciplina del regolamento comunale*) e provveditorato (*acquisto, conservazione e distribuzione di quanto occorre per il funzionamento degli uffici e dei servizi e manutenzione arredi, spese generali relative agli automezzi comunali, che non rientrano nella specifica competenza dei Responsabili di Area es. cancelleria, stampati, abbonamenti, acqua e ecc.*).
- Istruzione (*trasporto e mensa scolastica, acquisto libri di testo, rapporti con le istituzioni scolastiche, estate ragazzi ecc.*) Cultura e Biblioteca
- Politiche giovanili – servizi socio-assistenziali (g*estiti in maniera diretta, in forma associata o mediante delega a enti terz*i)
- Associazionismo e volontariato
- Sport e turismo (manifestazioni)
- Concessioni cimiteriali
- Gestione economica personale ed ogni altro adempimento relativo (s*tatistiche, conto del personale, adempimenti relativi all’anagrafe degli incarichi del personale ed esterni – malattia ec*c.)
- Tenuta inventari beni comunali
- Gestione polizze assicurative
- Partecipazioni societarie
- Supporto agli uffici comunali per le attività di competenza nella fase di riscossione delle varie entrate; e per le attività di competenza nelle fasi di impegno e liquidazione delle varie spese - controllo di gestione -
- Privacy relativa alla gestione e trattamento dei dati inerenti i servizi e materie di propria competenza - statistiche - stipulazione contratti in rappresentanza dell’Ente inerenti i servizi ricadenti nell’area - Predisposizione regolamenti, proposte di deliberazioni inerenti le materie di competenza e rilascio pareri di regolarità tecnica e contabile e attestazione di copertura finanziaria.

Allegato “2”,

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI, E SPECIFICHE ISTRUZIONI AI SOGGETTI DESIGNATI

Il Titolare del trattamento, per il tramite del sottoscritto dirigente/P.O., ed in forza del principio di «responsabilizzazione», impartisce alla persona fisica designata e delegata al trattamento, e sopra indicata, le istruzioni a cui è obbligata ad attenersi, sotto la comminatoria delle sanzioni di legge e di contratto.

In particolare, nella gestione dei processi/procedimenti inerenti i servizi e funzioni a cui la persona fisica designata al trattamento è preposta e, più in generale, nello svolgimento dell’attività lavorativa presso detto Ufficio, la delega ad effettuare le operazioni di trattamento dei dati personali nell’ambito della suddetta attività, e descritte nel documento Registro delle attività di trattamento del Titolare, viene rilasciata con le seguenti istruzioni che costituiscono cogenti prescrizioni, anche ai fini della responsabilità personale e disciplinare:

- 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 nell’Ufficio di appartenenza, 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 la persona fisica designata e delegata al trattamento è preposta;
- 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, e 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 di creare banche dati nuove senza espressa autorizzazione del Titolare o del sottoscritto Dirigente / Responsabile di P.O.;
  - 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, nell’Ufficio 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 e 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;
    - ove si renda necessario, segnalare al sottoscritto Dirigente / Responsabile di P.O. la necessità di adeguamento, correzione ed integrazione della modulistica in uso all'Ufficio;
    - conservare, nel rispetto del principio di accountability, tutte le versioni delle informative in uno specifico archivio interno cartaceo e telematico e di 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. In particolare, qualora riceva richieste provenienti dagli interessati, finalizzate all'esercizio dei propri diritti, dovrà:
        - darne tempestiva comunicazione al Dirigente / Responsabile di P.O., allegando copia delle richieste ricevute;
        - coordinarsi, ove necessario e per quanto di propria competenza, con il Dirigente / Responsabile di P.O. ovvero con le altre funzioni interne designate dal Titolare per gestire le relazioni con gli Interessati;
- seguire i seminari d'informazione e formazione in materia di protezione dei dati personali, obbligatori alla luce delle nuove disposizioni del GDPR ed a sostenere i relativi test finali finalizzati alla verifica dell'apprendimento;
- segnalare al sottoscritto Dirigente / Responsabile di P.O., con tempestività, eventuali anomalie, incidenti, furti, perdite accidentali di dati connessi con una ricaduta sul trattamento dei dati personali, al fine di attivare le procedure di comunicazione delle violazioni di dati all'Autorità di controllo ed ai soggetti autorizzati (istituto del c.d. data breach o violazione di dati personali);

- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a propria disposizione ed in particolare a collaborare nelle comunicazioni di violazioni di dati personali, negli adempimenti della valutazione di impatto e consultazione preventive;
- assistere il Titolare del trattamento nella tenuta del registro delle attività di trattamento istituito ai sensi dell'articolo 30 del GDPR, tenendo conto della natura del trattamento e delle informazioni a propria disposizione;
- segnalare al sottoscritto Dirigente / Responsabile di P.O., con tempestività, eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle 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;
- effettuare la comunicazione dei dati esclusivamente ai soggetti indicati dal sottoscritto Dirigente / Responsabile di P.O. e secondo le modalità stabilite dal medesimo;
- mantenere, salvo quanto precisato al punto precedente, la massima 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;
- fornire al sottoscritto Dirigente / Responsabile di P.O., a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentirgli di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare del trattamento, nel suo complesso ed articolazioni, al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- nel caso di presenza di utenti, ospiti o personale di servizio, all'interno dell'Ufficio, sarà necessario:
    - che la persona non sia visibile dall'esterno;
    - non ammettere in ufficio altre persone se non espressamente richiesto e in accordo con l'utente con cui stiamo parlando;
    - apporre fuori dalla porta una targhetta o altro equivalente che indichi che è in corso un colloquio;
    - fare attendere in luoghi in cui non sono presenti informazioni riservate o dati personali;
    - evitare che l'utente esponga le proprie questioni personali prima di accedere all'ufficio (se necessario, spiegare alla persona la motivazione);
    - è importante che sulla scrivania vi siano solo informazioni neutre ed impersonali e, comunque, appartenenti alle categorie di cui agli articoli 9 e 10 del GDPR;
    - evitare di allontanarsi dalla scrivania o riporre i documenti ed attivare il salvaschermo del PC;
    - durante il colloquio non devono essere ricevute telefonate; se necessario, rispondere e rinviare a più tardi la conversazione telefonica. Se nell'ufficio è inserita una segreteria telefonica assicurarsi sempre che, in presenza di persone, il volume sia al minimo e che i messaggi eventualmente lasciati non possano essere sentiti;
    - assicurarsi che schedari e armadi che contengono dati personali siano chiusi a chiave quando siamo assenti dall'ufficio, salvo che sia possibile chiudere l'ufficio stesso;
    - bloccare l'accesso ad estranei dell'ufficio.

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 designata e delegata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

A) **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 Dirigente / 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) rivolgersi tempestivamente, per difficoltà o questione inerente la sicurezza, al competente Dirigente / Responsabile di P.O.;

6) 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;

7) 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.

B) **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 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 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 supposto e l'assistenza, in caso di difficoltà, dell'amministratore di sistema (se esistente) o del Dirigente/P.O. dell'Ufficio:

- 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.

C) 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.

D) 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.

E) **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 designata e delegata 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.).

F) 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;

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

4) 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;

5) 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;

6) 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;

7) 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 Dirigente / Responsabile di P.O.

G) **Software, 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 o figura analoga ovvero dal Dirigente / Responsabile di P.O.

2) non è consentito uti1izzare 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;

6) 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;

7) 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).

H) **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 (password) fornita per l'accesso al singolo PC;

2) 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;

3) 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;

4) 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;

5) è proibito tentare di acquisire i privilegi di Amministratore di sistema;

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

7) 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.).

I) Supporti esterni di memorizzazione

La persona fisica designata e delegata 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 dal sottoscritto Dirigente / Responsabile di P.O. 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 del Titolare o del sottoscritto Dirigente / Responsabile di P.O.
- 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 soggetto autorizzato è informato e consapevole che l'accesso e la permanenza nei sistemi informatici dell'Ente per ragioni estranee e comunque diverse rispetto a quelle per le quali è stato abilitato ed autorizzato, costituisce il reato di accesso abusivo ai sistemi informativi e può comportare inoltre sanzioni disciplinari, anche gravi.