COMUNE DI BELVEDERE MARITTIMO

"Via Maggiore Mistorni - 87021 Belvedere Marittimo (CS)"
Tel.: 0985.887411 - C.F.: 00346830789
PEC: belvederemarittimo.cs.segreteria@pec.it
Sito istituzionale: https://www.comune.belvedere-marittimo.cs.it/

REG. GENERALE N. 02/2021

DECRETO DEL COMISSARIO STRAORDINARIO CON POTERI DEL SINDACO

Numero 17965 - Del 03/12/2021

ATTO DI DESIGNAZIONE/AUTORIZZAZIONE

– Misure finalizzate alla corretta attuazione alle disposizioni del Regolamento (UE) 679/2016 e del D.Lgs. 196/2003 così come modificato e novellato dal D.Lgs. 101/2018 –

OGGETTO: Atto di individuazione e di nomina soggetti Autorizzati al trattamento dei dati personali, ai sensi degli art. 2 quaterdecies del D.Lgs. 196/2003 come novellato dal D.Lgs. 101/2018 e dell'art. 29 del Regolamento Europeo 679/2016 (GDPR)

IL COMISSARIO STRAORDINARIO CON POTERI DEL 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);

Visto il D.Lgs. 30 Giugno 2003, n.196 "Codice in materia di protezione dei dati personali";

Visto il D.Lgs. del 10 Agosto 2018 n.101 "Adeguamento al Regolamento UE 2016/679";

Visto il D.Lgs. 51/2018;

Visto il D.Lgs. 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale" e ss.mm.ii.;

Dato atto che il Comune di Belvedere Marittimo è Titolare dei trattamenti dei dati personali, effettuati sia con strumenti elettronici che senza l'ausilio di strumenti elettronici, necessari per lo svolgimento dei procedimenti amministrativi afferenti alle funzioni istituzionali affidate dalle fonti di diritto dell'Unione Europea e dello Stato italiano;

Rilevato che, ai fini dell'osservanza delle disposizioni contenute nelle sopracitate normative nazionali ed europee, vanno 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 del D.Lgs. 101/2018 e della modificata definizione di Responsabile del trattamento, si rende necessario procedere all'adeguamento degli atti di nomina, al

fine di attribuire specifici funzioni e compiti connessi al trattamento 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 … […]

Dato atto in particolare che il GDPR e la normativa nazionale di adeguamento, consentono comunque di mantenere le funzioni ed i compiti assegnati a figure interne all'Ente che, ai sensi del Codice nel testo previgente all'adeguamento al GDPR, ma non anche ai sensi del GDPR, potevano essere definiti come "*Responsabili interni*" del trattamento, In particolare, 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".

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/Area/Ufficio;

Appurato che l'ordinamento interno del Titolare, così come si ricava dallo Statuto e dai Regolamenti in vigore, risulta compatibile con i compiti e funzioni delegate;

Visto lo Statuto di questo Ente;

DECRETA

La nomina, con decorrenza dalla data del presente provvedimento, del Segretario comunale e dei Responsabili di Posizioni Organizzative quali Designati al trattamento dei dati personali, ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003 come novellato dal D.Lgs. 101/2018

NOMINA

1. Tutti i dipendenti/collaboratori stabili del Titolare (compresi i Designati al trattamento) quali "Persone Autorizzate al trattamento" (ex art. 29 del GDPR) per i trattamenti di tutti i dati necessari per l'espletamento delle mansioni ricoperte all'interno dell'Ente (con esclusione dei soggetti che nell'espletamento delle mansioni attribuite non trattano dati personali).

DECRETA INOLTRE

1) **DI PUNTUALIZZARE** che i compiti e le funzioni a tal fine assegnate sono analiticamente elencate in calce 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 dovere di svolgere i compiti le funzioni attribuite dal Titolare;

2) **DI DARE ATTO**, altresì, che:

- tale ruolo ha validità per l'intera durata del rapporto, nonché acquisterà efficacia nei confronti dei sostituti che ricopriranno uguale ruolo;
- 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.

3) **DI DARE ATTO** che il presente provvedimento sostituisce gli atti a suo tempo adottati:

NOTIFICA, COMUNICAZIONE E PUBBLICAZIONE DEL PRESENTE DECRETO

Il presente Decreto dovrà essere:

- Pubblicato all'Albo Pretorio on-line e nella sezione "Amministrazione trasparente" in apposita sezione dedicata alla Protezione dei dati personali (c.d. "Privacy" o "Altri contenuti") del sito web istituzionale di questo Ente. La stessa pubblicazione avrà valore di notifica ai destinatari;
- Comunicato al Responsabile della Protezione dei Dati - DPO;
- Consegnato successivamente alla data di entrata in vigore (per presa visione), a chiunque intratterrà rapporti con l'Ente (Neo-assunti, Tirocinanti, Stagisti, Volontari e simili).

Lì, 03/12/2021

IL COMISSARIO STRAORDINARIO

Dott.ssa Regina Antonella Bardari

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

SOTTO IL PROFILO ORGANIZZATIVO (SOLO DESIGNATI AL TRATTAMENTO)

- collaborare con il Titolare del trattamento per l'inserimento degli obiettivi strategici e operativi del sistema di sicurezza e di protezione dei dati personali nel Piano degli Obiettivi e delle Performance nonché nel DUP e negli altri strumenti di programmazione;
- identificare Contitolari, Responsabili e Sub Responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere gli accordi interni ed i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi ai contitolari ed ai responsabili;
- acquisire, se necessario, dai Contitolari, Responsabili e Sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi risultano autorizzate al trattamento ed a compiere le relative operazioni;
- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative e organizzative che impattano sui trattamenti, della ricognizione degli stessi al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;
- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati;
- effettuare, prima di procedere al trattamento, quando questo può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una Valutazione dell'Impatto del trattamento sulla Protezione dei Dati personali (DPIA);
- mettere in atto le misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
  a) la pseudonimizzazione e la cifratura dei dati personali;
  b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
  d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- mettere in atto le misure tecniche ed organizzative per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, fermo restando che:
- proporre e suggerire al Titolare misure tecniche ed organizzative ritenute necessarie a garantire la protezione dei dati dal trattamento, in relazione ai trattamenti della struttura organizzativa di competenza;
- contribuire alla tenuta del Registro delle Attività di trattamento in relazione ai trattamenti della struttura organizzativa di competenza;
- cooperare, su richiesta, con il RPD/DPO e con l'Autorità di controllo nell'esecuzione dei rispettivi compiti;
- in caso di violazione dei dati personali, collaborare con il Titolare, il RPD/DPO nel processo di notifica della violazione all'Autorità di controllo competente senza ingiustificato ritardo e, comunque, entro 24/72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia

improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;

- in caso di violazione dei dati personali, comunicare la violazione all'Interessato senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- prima di procedere al trattamento, consultare l'Autorità di controllo qualora la Valutazione d'Impatto sulla Protezione dei Dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
- assicurarsi che il RPD/DPO sia tempestivamente ed adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- sostenere il RPD/DPO nell'esecuzione dei compiti assegnati, fornendogli le risorse necessarie per assolvere tali compiti, per accedere ai dati personali ed ai trattamenti e per mantenere la propria conoscenza specialistica;
- documentare e tracciare, per iscritto, ed essere in grado di provare, in caso di richiesta dell'Autorità di controllo, l'attuazione del sistema di sicurezza finalizzato alla protezione dei dati personali;
- controllare e monitorare la conformità dell'analisi, della valutazione dei rischi e della valutazione di impatto nonché controllare e monitorare la conformità del trattamento dei rischi al contesto normativo, regolamentare, gestionale, operativo e procedurale, con obbligo di tempestiva revisione in caso di rilevazioni di non conformità o di scostamenti;
- conformare il trattamento ai pareri ed indicazioni del RPD/DPO e dell'Autorità di controllo nonché alle linee guida ed ai provvedimenti dell'Autorità di controllo;
- formulare proposte, in occasione dell'approvazione/aggiornamento annuale degli strumenti di pianificazione e programmazione, volte ad implementare il sistema di sicurezza e ad elevare il livello di protezione degli interessati;
- attuare e partecipare alla formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati;
- promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione come valore da integrare in ogni processo/procedimento;
- effettuare ogni ulteriore attività, anche se non espressamente indicata in precedenza e necessaria per la integrale attuazione del GDPR e della normativa di riferimento.

SOTTO IL PROFILO DEL TRATTAMENTO DI DATI PERSONALI (PER TUTTI):

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 Designata 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.

B) 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;

C) 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 Dirigente 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 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 e togliere la smart card dall'apposito alloggiamento.

E) 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.).

F) Posta elettronica

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

- ✓ 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.

G) **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).

H) **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.).

I) 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;