COMUNE DI ACQUI TERME

Decreto n. 1 del 28 febbraio 2019

Oggetto: Misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n. 2016/679 – Atto di designazione dell'Amministratore di sistema in relazione al trattamento dei dati personali, e conseguente attribuzione al soggetto designato di specifici compiti e funzioni, con delega all'esercizio ed allo svolgimento degli stessi secondo analitiche istruzioni impartite.

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;

CONSIDERATO che, conformemente alle disposizioni del GDPR, e della normativa interna di adeguamento - 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. 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*" - 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;

DATO ATTO che si rende necessario procedere alla designazione della persona fisica dedicata alla gestione ed alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di

dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali, secondo quanto previsto nel Provvedimento del Garante per la protezione dei dati personali sull'Amministratore di sistema del 27 novembre 2008;

CONSIDERATO che nel GDPR non sembra ci sia un chiaro riferimento alla figura dell'amministratore di sistema nel processo di trattazione e custodia dei dati, pur trattandosi di una figura implicitamente richiamata, in alcune norme, per le sue specifiche competenze tecniche, laddove al titolare del trattamento e/o all'eventuale responsabile nominato, spetta il compito di mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32);

VALUTATA in ogni caso l'esigenza per questa amministrazione, stante la complessità dell'apparato tecnologico esistente, di procedere con l'individuazione di tale figura professionale, attribuendole specifici compiti e funzioni spettanti al Titolare ed analiticamente elencati nel documento allegato al presente atto, ferma restando l'imputazione della responsabilità conseguente al trattamento in capo al Titolare medesimo;

APPURATO che l'ordinamento interno del Titolare, così come si ricava dallo Statuto e dai Regolamenti in vigore, risulta compatibile con la delega di compiti e funzioni a Dirigenti e Responsabili di P.O.;

CONSIDERATA la struttura organizzativa e l'organigramma funzionale degli Uffici e dei Servizi di questo Ente;

DATO ATTO che presso l'Ente è preposto quale Responsabile del Sistema Informatico il Sig. Pier Guido Colla, di cui è stata anche verificata l'idoneità rispetto alle caratteristiche di esperienza, capacità e affidabilità richieste dalle vigenti disposizioni per adempiere agli obblighi in materia di sicurezza del trattamento informatico dei dati e per svolgere attività di gestione tecnica del sistema informatico;

VISTO lo Statuto Comunale;

VISTO il vigente Regolamento sull'Ordinamento degli Uffici e dei Servizi;

DECRETA

1. di designare, con decorrenza dalla data di ricezione del presente provvedimento, il Sig. Colla Pier Guido che opera sotto la diretta autorità del Titolare, quale persona fisica a cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali, con specifico riferimento alla gestione ed alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali, 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 Sig. Colla

Pier Guido, i compiti e le funzioni analiticamente elencate nel documento allegato al presente decreto per divenirne parte integrante e sostanziale, con facoltà di successiva integrazione e/o modificazione, dando atto che l'attribuzione di compiti e funzioni inerenti il trattamento dei dati personali non implica l'attribuzione di compiti e funzioni ulteriori rispetto a quelli propri della qualifica rivestita, ma conferisce soltanto il potere/dovere di svolgere i compiti e le funzioni attribuite dal Titolare;

3. di delegare, per effetto di quanto sopra indicato e con decorrenza dalla data di ricezione del presente provvedimento, al Sig. Colla Pier Guido l'esercizio e lo svolgimento di tutti i compiti e di tutte le funzioni attribuite dal Titolare, ed analiticamente elencate nel documento allegato al presente decreto per divenirne parte integrante e sostanziale, con facoltà di successiva integrazione e/o modificazione;

4. di dare atto che il suddetto assume, con decorrenza dalla data di ricezione del presente atto di designazione, attribuzione e delega, il ruolo di Amministratore di sistema con delega a svolgere i compiti e le funzioni attribuiti dal Titolare medesimo;

5. di dare atto, altresì, che:
   - tale ruolo ha validità per l'intera durata del rapporto del rapporto di lavoro;
   - tale ruolo viene a cessare al modificarsi del rapporto di lavoro;
   - tale ruolo viene a cessare in caso di revoca espressa;
   - tale ruolo non consente l'attribuzione ad altri soggetti di poteri e compiti qui previsti;
   - al cessare di tale ruolo, rimane inibito e comunque non autorizzato ogni ulteriore esercizio dei compiti e delle funzioni di 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;

6. di disporre la pubblicazione del presente provvedimento all'albo pretorio on line e nella sezione Amministrazione trasparente;

7. di disporre la comunicazione personale, con rilascio di apposita dichiarazione di ricevimento del presente atto.

Acqui Terme, 28 febbraio 2019

CITTA' DI ACQUI TERME - AL

IL SINDACO
Lorenzo Lucchini

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI ALL'AMMINISTRATORE DI SISTEMA E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI

L'Amministratore di Sistema è la figura professionale che si occupa della gestione e della manutenzione del sistema comunale di elaborazione e delle sue componenti. Egli opererà nei seguenti ambiti:
- gestione dei sistemi operativi;
- gestione delle credenziali di autenticazione;
- gestione dei data base;
- gestione delle reti;
- gestione degli strumenti- e apparati di sicurezza, comprese le copie dì sicurezza e ripristino;
- manutenzione hardware e software;
- gestione dei locali.

La sua opera dovrà garantire alla rete informativa del Comune un buon grado di:
- disponibilità, intesa come capacità della rete di rendere disponibili le risorse nel momento in cui vengono chieste dall'utenza;
- efficienza, intesa come funzionamento ottimale delle risorse da parte dell'utenza;
- flessibilità, intesa come capacità della rete di adeguarsi al mutare delle esigenze;
- scalabilità, intesa come capacità della rete di crescere in modo adeguato ed a costi ridotti;
- robustezza, intesa come capacità intrinseca della rete di resistere a guasti più o meno invasivi;
- sicurezza, intesa come capacità della rete di rilevare e confinare anomalie e problemi di sicurezza generati dall'interno o provenienti dall'esterno;
- compliance, intesa come aderenza alle normative di legge finalizzate al corretto uso delle risorse telematiche

L'Amministratore nella sua opera dovrà:
1) installare e configurare nuovo hardware/software sia lato client sia lato server;
2) adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza del sistema informativo, verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi;
3) pianificare e comunicare preventivamente all'utenza tutte le attività tecnico sistemistiche che possano compromettere la continuità operativa dei sistemi informatici. Fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti. 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;
4) applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze dell'Ente;
5) monitorare l'infrastruttura informatica attraverso l'analisi dei log, identificando e prevenendo potenziali problemi;
6) garantire che le risorse vengano utilizzate dagli utenti che ne abbiano effettivamente diritto, utilizzando gli opportuni meccanismi di identificazione e autenticazione. Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione. L'Amministratore di sistema adotta sistemi idonei per garantire la registrazione degli accessi logici al sistema informativo. Le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste. I sistemi ed i dispositivi infrastrutturali ritenuti vitali e critici (per sensibilità dei dati contenuti o in quanto connessi direttamente alla continuità di servizi) dovranno prevedere anche la registrazione degli eventi. Per un miglior controllo e governo

dell'infrastruttura informatica dell'Ente, sarà opportuno estendere la registrazione a tutti gli eventi di tutti i dispositivi collegati. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a 6 mesi. Gli access log possono essere cancellati solamente alla scadenza dei 6 mesi. La conservazione degli access log può essere on site o in outsourcing. In ogni caso dovrà essere in linea con le regole tecniche contenute nella deliberazione CNIPA n. 11/2004 e successive modificazioni;

7) vigilare sugli interventi informatici diretti al sistema informatico complessivo del Comune effettuati da vari operatori esterni;
8) provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego;
9) adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate. L'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
10) documentare le operazioni effettuate, le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi;
11) la documentazione interna al proprio ufficio, in particolare la documentazione relativa all'infrastruttura di rete, alla configurazione dei sistemi o degli applicativi, alle impostazioni o abilitazioni degli utenti, deve essere conservata in luogo sicuro, preferibilmente non accessibile in rete. L'accesso a detta documentazione è consentito solamente al personale nominato Amministratore di Sistema, per il solo tempo necessario alla consultazione e all'aggiornamento. E' vietato trasportare la Documentazione Interna del Settore Informatica in qualsiasi formato o media all'esterno dell'Ente. Il divieto include l'invio di mail/fax/lettere contenenti documentazione anche parziale, la compilazione o la risposta ad interviste/indagini di mercato effettuate tramite telefono/fax/lettera. Gli account e le relative password di livello Amministratore di Sistema non devono essere rivelate a nessuno per nessun motivo. E' vietato trasmettere in qualsiasi formato anche criptato dette informazioni. In caso di perdita di segretezza di una password di livello Amministratore di Sistema, è necessario effettuarne immediatamente la modifica e verificare che non siano stati creati nel frattempo nuovi utenti o modificati profili di autorizzazione.

SOTTO IL PROFILO ORGANIZZATIVO E FUNZIONALE:

- svolgere un ruolo di primaria interfaccia nella scelta delle dotazioni informatiche, nessuna esclusa, quali hardware di qualsiasi genere, software e qualsiasi altro dispositivo elettronico, e di tutti i processi tecnologici dell'Ente, partecipando ai processi decisionali dei singoli servizi, che dovranno acquisire parere dell'Amministratore di rete sulle suddette dotazioni informatiche. Coadiuvare i Dirigenti / Responsabili di P.O. nella definizione e nell'organizzazione degli applicativi usati per la gestione dei singoli uffici;
- svolgere un ruolo di primaria interfaccia nel caso di incidenti/malfunzionamenti di qualsiasi genere che riguardino la rete, le attrezzature informatiche e l'utenza e preoccuparsi di erogare una corretta informazione verso gli utenti esterni; dovrà inoltre supportare il processo di indagine e diagnosi dei problemi ed essere in grado di produrre le necessarie informazioni a tal riguardo;
- collaborare con gli altri Dirigenti / Responsabili di P.O., designati e delegati e con il Segretario/Direttore per l'elaborazione degli obiettivi strategici ed operativi del sistema di sicurezza e di protezione dei dati personali da sottoporre all'approvazione del Titolare;
- collaborare con gli altri Dirigenti / Responsabili di P.O., designati e delegati e con il Segretario/Direttore per l'elaborazione della pianificazione strategica del sistema di

sicurezza e di protezione dei dati personali attraverso l'elaborazione di un Piano per la sicurezza/protezione, da sottoporre all'approvazione del Titolare;

- collaborare con gli altri Dirigenti / Responsabili di P.O. designati e delegati e con il Segretario/Direttore per l'elaborazione e l'aggiornamento delle procedure necessarie al sistema di sicurezza e, in particolare per la procedura da utilizzare in caso di c.d. data breach, da sottoporre all'approvazione del Titolare;
- 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 della Performance/PDO nonché nel DUP e negli altri strumenti di pianificazione del Titolare;
- 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 dai contitolari, responsabili e sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi contitolari, responsabili e sub responsabili risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni;
- identificare e designare, per iscritto ed in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura organizzativa di competenza, le persone fisiche della struttura organizzativa medesima, che operano sotto la diretta autorità del Titolare ed attribuire alle persone medesime specifici compiti e funzioni inerenti al trattamento dei dati, conferendo apposita delega per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento, impartendo a tale fine analitiche istruzioni e controllando costantemente che le persone fisiche designate, delegate e autorizzate 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».
- ove ciò si renda necessario, segnalare al Titolare l'esigenza che vengano designati amministratore di sistema anche altri soggetti appartenenti al proprio ufficio o servizio, al fine di consentire la pronta reperibilità ed esercizio della funzione. Spetta in ogni caso al Titolare la relativa nomina e la predisposizione di apposito elenco nominativo dei soggetti designati;
- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti nella struttura organizzativa di competenza, in correlazione con i processi/procedimenti svolti dall'Ufficio, da sottoporre all'approvazione del Titolare;
- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa, con obbligo di sottoporre l'aggiornamento all'approvazione del Titolare;
- 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, da sottoporre all'approvazione del Titolare;
- 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;

- mettere in atto le misure tecniche ed organizzative adeguate, identificate dal Titolare, funzionali 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 adeguate, identificate dal Titolare per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, fermo restando che:
  a) tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità;
  b) dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica
- 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 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;
- collaborare con il Titolare per l'inserimento dei rischi di corruzione, illegalità e degli illeciti in materia di trattamento di dati personali negli aggiornamenti annuali al PTPC e collaborare al RPC per le segnalazioni degli illeciti relativi al trattamento dei dati;
- documentare tutte le attività e gli adempimenti delegati e, in ogni caso, tracciare documentalmente l'intero processo di gestione dei rischi e del sistema di sicurezza e protezione;

- 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;
- tracciare documentalmente le attività di controllo e monitoraggio mediante periodici report/resoconti/referti da sottoporre al Titolare ed al RPD/DPO;
- 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, di informatica giuridica, e di diritto;
- 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:

Nello svolgere le proprie funzioni, che comportino un trattamento di dati personali, l'Amministratore di sistema 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 l'Amministratore di sistema 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 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 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 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:

- **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) 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) utilizzare sempre il proprio codice di accesso personale ai dispositivi elettronici ed alle applicazioni software, 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:
  - 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 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.).

- **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;

- **Software, applicazioni e servizi esterni**
  1) non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
  2) 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;
  3) 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;

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

  6) 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 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. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
  - 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.

Dichiarazione di ricevimento dell'atto di designazione, autorizzazione e delega e di impegno all'assunzione ed all'esercizio dei compiti, delle funzioni e delle responsabilità attribuite e delegate riferita al Decreto Sindacale n. 1 del 28 febbraio 2019 avente per oggetto " Misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n. 2016/679 – Atto di designazione dell'Amministratore di sistema in relazione al trattamento dei dati personali, e conseguente attribuzione al soggetto designato di specifici compiti e funzioni, con delega all'esercizio ed allo svolgimento degli stessi secondo analitiche istruzioni impartite".

Il sottoscritto Amministratore di sistema, Sig. Pier Guido Colla,

DICHIARA

1. di aver ricevuto il sovrascritto atto di designazione, attribuzione e delega di funzioni e responsabilità per il trattamento dei dati personali nell'ambito della struttura organizzativa alla quale è preposto;
2. di aver attentamente letto e compreso il contenuto di tale atto, e di impegnarsi ad attuare la delega;
3. di dare atto che l'obbligo di riservatezza correlato al ruolo assunto va osservato anche per il tempo successivo alla cessazione dell'incarico medesimo.

ACQUI 1/3/2019

L'Amministratore di sistema

Pier Guido Colla