

Dipartimento di ..... – Struttura .....

PROVVEDIMENTO DI NOMINA PROT. N. \_\_\_\_ DEL \_\_\_\_/\_\_\_\_/\_\_\_\_

**INDIVIDUAZIONE DEI LAVORATORI IN FORZA ALLA STRUTTURA IN INTESTAZIONE QUALI PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI, ai sensi degli artt. 4, par. 1, punto 10), 29, 32, par. 4, RGPD 2016/679 e art. 2-quaterdecies, comma 2, del D. Lgs. n. 196/03 e ss.mm.ii.**

**Il Responsabile della Struttura Complessa – della Struttura Semplice – del Dipartimento**, all'uopo individuato con Provvedimento della Direzione Generale, Titolo, Nome e Cognome \_\_\_\_\_, ai sensi del **Regolamento UE n. 2016/679 (in seguito, "GDPR")** e del Regolamento interno per l'attuazione del Regolamento Europeo adottato dalla ASL Gallura (Azienda socio-sanitaria locale) con Provvedimento del Direttore Generale n. \_\_\_\_ del \_\_\_\_/\_\_\_\_/\_\_\_\_, viste le disposizioni di cui all'art. 2-quaterdecies, comma 1 del D. Lgs. 196/03, in qualità di persona fisica all'uopo designata con Provvedimento del Direttore Generale n. \_\_\_\_ del \_\_\_\_/\_\_\_\_/\_\_\_\_, dovendo provvedere all'individuazione degli autorizzati al trattamento dei dati per le attività aziendali,

Premesso che:

- **in data 25 maggio 2018**, è divenuto definitivamente applicabile in via diretta in tutti i Paesi UE 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 (Regolamento generale sulla protezione dei dati)*» (di seguito **RGPD**);
- **in data 10 agosto 2018** è stato adottato il D. Lgs. n. 101/18, entrato in vigore il 19 settembre 2018, di modifica del D. Lgs. 196/03 recante disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati)*»;
- **in data 02 settembre 2020** sono state adottate dal Comitato Europeo per la protezione dei dati le Linee Guida 07/2020 sui concetti di "Controller" e "Processor" equivalenti rispettivamente al Titolare del trattamento ed al Responsabile del trattamento dei dati, al fine di definire a chi debbano essere attribuite le responsabilità sulla conformità dei trattamenti dei dati personali effettuati e come detti soggetti possano esercitare i loro diritti sul piano pratico. La finalità delle Linee Guida 07/2020 è garantire l'uniforme applicazione della disciplina su Titolari e Responsabili all'interno dell'Area Economica Europea;
- ai sensi dell'art.4, paragrafo 1, punto 7), RGPD 2016/679, per Titolare del trattamento si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o l'organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Nel caso di una Pubblica Amministrazione, il Titolare del trattamento dei dati è l'Azienda nel suo complesso;
- Con Provvedimento n. \_\_\_\_ del \_\_\_\_/\_\_\_\_/\_\_\_\_ il Direttore Generale, nella sua qualità di legale rappresentante dell'Azienda, ha individuato il sottoscritto quale Responsabile di Struttura, espressamente designato allo svolgimento di specifici compiti connessi al trattamento dei dati personali in conformità alle previsioni di cui all'art. 2-quaterdecies, comma 1, del D. Lgs. n. 196/2003;
- considerato che l'art. 4, paragrafo 1, punto 10) RGPD 2016/679 prevede espressamente l'esistenza di "*persone autorizzate al trattamento dei dati personali*" sotto l'autorità diretta del Titolare del trattamento;
- l'art. 29, RGPD, prevede che "*chiunque abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento*";

- il richiamato art. 29, RGPD, prevede che le operazioni di trattamento possano essere effettuate solo da soggetti che operino sotto la diretta autorità del Titolare, attenendosi alle istruzioni impartite;
- l'art. 2-quaterdecies, comma 2, del D. Lgs. n. 196/2003 aggiornato al D. Lgs. n. 101/2018, stabilisce che il Titolare del trattamento individua "le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta";
- che con Delibera del Direttore Generale n. \_\_ del \_\_/\_\_/\_\_\_\_ è stata approvata la macrostruttura dell'Azienda e la sua organizzazione;
- ad ogni Dirigente/Direttore in forza, ciascuno nell'ambito della direzione della Struttura di diretta competenza, sono attribuiti compiti e funzioni connessi al trattamento, tra i quali quelli relativi alla individuazione delle persone fisiche che sotto l'autorità diretta svolgano attività che comportino trattamento di dati personali;
- si rende necessario procedere alla formale ed espressa individuazione delle persone fisiche autorizzate al trattamento dei dati personali, nell'ambito della Struttura di assegnazione, con particolare riferimento alle Banche Dati trattate da detta Struttura e dalle sue articolazioni funzionali ove presenti;
- le persone fisiche autorizzate, effettueranno il trattamento dei dati, attenendosi scrupolosamente alle istruzioni impartite dal Titolare del trattamento;

Visto:

- le schede di rilevazione dei singoli procedimenti amministrativi e dei processi di pertinenza della Struttura, qui richiamate integralmente per costituire parte integrante e sostanziale del presente atto;
- il censimento analitico delle Banche Dati cartacee e/o informatiche trattate dalla Struttura per la gestione dei procedimenti amministrativi e dei processi di competenza, qui richiamato integralmente per fare parte integrante e sostanziale del presente atto;
- l'elenco nominativo del personale assegnato alla Struttura e pertanto autorizzati a trattare i dati relativi ai singoli procedimenti amministrativi di competenza dell'Ufficio/Servizio di assegnazione;

ritenuto, di dover procedere all'individuazione delle persone autorizzate al trattamento dei dati ai sensi dell'art. 2-quaterdecies, comma 2 del D. Lgs. n. 196/2003;

tutto ciò premesso:

**DISPONE**

**di autorizzare espressamente al trattamento dei dati personali** della Struttura \_\_\_\_\_ i Signori:

Nome Cognome	Dipendente	Convenzione	Tirocinante	Inquadramento	Procedimenti, processi e trattamenti autorizzati

In ottemperanza al RGPD, che disciplina la protezione delle persone fisiche con riferimento al trattamento dei dati personali, le SS. LL. sono autorizzate a trattare i dati personali e le categorie particolari di dati di cui agli artt. 9 e 10 del RGPD, strettamente necessari per l'istruttoria e la definizione dei procedimenti di competenza della Struttura di assegnazione, secondo le indicazioni di seguito dettagliate.

**I dipendenti, individuati quali Persone Autorizzate al trattamento dei dati sono legittimati:**

- a trattare i dati personali di cui vengano a conoscenza nell'ambito dello svolgimento della propria attività istituzionale in modo lecito e secondo correttezza, secondo i principi di cui all'art. 5, paragrafo, 1 RGPD;
- ad effettuare le operazioni di trattamento di cui all'art. 4, Paragrafo 1, n. 2 del RGPD per lo svolgimento delle funzioni istituzionali di competenza della Struttura alla quale sono stati assegnati;
- ad accedere unicamente alle banche dati strettamente necessarie per l'espletamento delle funzioni istituzionali proprie dei procedimenti di competenza della Struttura alla quale sono stati assegnati.

**I dipendenti individuati quali Persone Autorizzate al trattamento dei dati devono:**

- per l'accesso alle banche dati informatiche, utilizzare sempre le proprie credenziali personali di accesso, mantenendole riservate, evitando di operare su terminali altrui e avendo cura di non lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati o non consentiti e di rendere possibile, in qualunque momento, l'individuazione dell'autore materiale del trattamento;
- conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che detti supporti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- mantenere la massima riservatezza ed il dovuto riserbo sui dati personali dei quali si venga a conoscenza nello svolgimento delle funzioni istituzionali con riferimento alla gestione dei procedimenti di competenza;
- custodire e controllare i dati personali affidati affinché siano ridotti i rischi di distruzione o perdita anche accidentale degli stessi, accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta;
- evitare di creare banche dati nuove senza autorizzazione espressa del Responsabile di riferimento;
- fornire al Titolare del trattamento o alle persone dal Titolare espressamente designate, tutte le informazioni relative all'attività svolta, al fine di consentire una efficace attività di controllo;
- conservare i dati rispettando le misure di sicurezza predisposte dall'Azienda, in conformità alle disposizioni impartite dal Responsabile designato, come di seguito dettagliate.

**Con riferimento all'utilizzo della postazione di lavoro assegnata in uso:**

- Il Personal Computer (PC) affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi ulteriori di manutenzione e minacce alla sicurezza dei dati personali trattati dall'Azienda.
- I dipendenti devono custodire la propria strumentazione in modo diligente, segnalando con tempestività ogni danneggiamento, avaria, furto o smarrimento al Responsabile designato.
- L'accesso a ciascun PC è protetto da credenziale di autenticazione costituita da una User ID (codice per l'identificazione dell'autorizzato) associata a una PASSWORD riservata (parola chiave), conosciuta esclusivamente dal medesimo autorizzato.
- Le persone autorizzate al trattamento dei dati sono responsabili della custodia e dell'utilizzo diligente e consapevole delle proprie credenziali di autenticazione che devono essere gestite attenendosi alle istruzioni fornite dai servizi informativi aziendali.

- L'autenticazione al PC e/o agli applicativi dovrà avvenire mediante utilizzo di sistemi di autenticazione a due fattori ovvero associati a procedure OTP; nelle more dell'attivazione di detti sistemi, idonei a garantire la sicurezza del trattamento, la password deve:
  - ☐ essere generata autonomamente dall'autorizzato al trattamento, abilitato alla consultazione delle banche dati necessarie per l'espletamento delle funzioni istituzionali proprie dei procedimenti di competenza, all'atto del primo accesso ed essere mantenuta segreta con divieto assoluto di comunicazione a terzi o di condivisione;
  - ☐ essere di almeno 8 caratteri, ma deve essere consentita una lunghezza massima di almeno 64 caratteri con utilizzo di tutti i caratteri ASCII (RFC 20);
  - ☐ non presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti;
  - ☐ non contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;
  - ☐ non essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniero) o che si riferiscano ad informazioni personali;
  - ☐ non essere memorizzata in funzioni di log-in automatico, come per esempio il completamento;
  - ☐ non essere associata a c.d. "domande di sicurezza";
  - ☐ poter essere gestita mediante la funzionalità di "incolla" in fase di inserimento per facilitare l'uso dei gestori di password (i password manager), ampiamente consigliati perché aumentano la probabilità che gli utenti scelgano password più forti;
  - ☐ poter essere inserita in chiaro, evitando l'utilizzo di punti o asterischi;ove tecnicamente possibile, i requisiti di cui ai punti sopra indicati sono imposti da meccanismi automatici del sistema;
- ☐ la password deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- ☐ la persona autorizzata è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;
- ☐ qualora, in caso di prolungata assenza o impedimento della persona autorizzata, si verificasse la necessità di accedere ai dati ed agli strumenti elettronici per esigenze di operatività e di sicurezza del sistema, il Titolare o la persona fisica dal Titolare espressamente designata provvede ad eseguire l'accesso autonomamente utilizzando le proprie credenziali di autenticazione – in quanto configurate secondo un profilo di autorizzazione sovraordinato rispetto a quello delle persone autorizzate, propri subordinati gerarchici – redigendo un verbale di operazioni compiute. In tal modo è garantita la piena tracciabilità dell'accesso che sarà comunque registrato mediante i file di log. Al rientro in servizio della persona autorizzata assente ovvero impedita, il Titolare o la persona fisica dal Titolare espressamente designata, provvederà ad informarlo dell'accaduto consegnandogli copia del verbale di operazioni compiute;
- ☐ le credenziali di autenticazione individuali per l'accesso al profilo dell'utente, all'elaboratore ovvero alle applicazioni, non devono mai essere condivise tra più utenti (anche se Autorizzati al trattamento). Se un dipendente dovesse avere la necessità di trattare gli stessi dati o di usare le stesse procedure alle quali può accedere un collega, dovrà richiedere, al Titolare del trattamento ovvero all'Amministratore di Sistema, che

gli siano assegnate le proprie credenziali di autenticazione, dotate dei privilegi necessari all'accesso ai dati o ai servizi richiesti;

☐ se la persona autorizzata sospetta che le proprie credenziali di autenticazione abbiano perso il requisito della segretezza (ad es. perché crede che queste siano conosciute anche da altri colleghi) è tenuto immediatamente a procedere al cambio della propria password, come espressamente previsto dalla pubblicazione NIST SP 800-63 "Digital Identity Guidelines" alla quale si rinvia integralmente.

- Il dipendente autorizzato al trattamento dei dati, preso atto che, la conoscenza della password da parte di terzi consente agli stessi l'accesso all'elaboratore, l'utilizzo dei relativi dati nonché l'accesso ai dati cui il medesimo dipendente è abilitato, con possibilità di gestione degli stessi (visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della propria posta elettronica, uso indebito di servizi ecc.), si impegna a:
  - non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro in particolar modo per quanto riguarda l'accesso ad Internet ed ai servizi di posta elettronica;
  - non lasciare incustodita ed accessibile la propria postazione una volta che sia avvenuta l'autenticazione con le proprie credenziali;
  - conservare e custodire la password nella massima riservatezza e con la massima diligenza;
  - non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti casualmente conoscenza;
  - mantenere la corretta configurazione del proprio elaboratore non alterando le componenti hardware e software predisposte allo scopo né installando ulteriori software non autorizzati.
- Qualunque azione o attività attuata mediante l'utilizzo del codice identificativo e della password assegnate, è attribuita in via esclusiva al dipendente assegnatario delle credenziali di autenticazione che sarà chiamato a rispondere delle attività eseguite.
- Il dipendente è civilmente responsabile di qualsiasi danno arrecato all'Azienda, all'internet provider e/o a terzi in violazione di quanto espressamente previsto dalla norma e di quanto indicato nel presente provvedimento.
- Il dipendente può essere chiamato a rispondere, oltre che per i propri fatti illeciti, anche per quelli commessi da chiunque utilizzi il suo codice identificativo e la sua password, con particolare riferimento all'immissione in rete di contenuti critici o idonei ad offendere l'ordine pubblico e il buon costume così come definiti dalla giurisprudenza più recente.
- La violazione delle presenti disposizioni può comportare infine l'applicazione delle sanzioni disciplinari previste dal vigente Contratto Collettivo di Lavoro, rimanendo ferma ogni ulteriore forma di responsabilità personale.
- Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile designato e dell'Amministratore di Sistema dell'Azienda. In caso di necessità di acquisto o di dotazione di programmi applicativi e procedure, sarà necessario preventivamente richiedere e acquisire l'autorizzazione in forma scritta da parte dell'amministratore di Sistema dell'Azienda, per garantirne la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e della Rete.
- Non è consentito ai dipendenti modificare le caratteristiche impostate sui PC assegnati, le configurazioni della rete LAN presente nella sede dell'Azienda e la configurazione del Browser per la navigazione, salvo esplicita autorizzazione dell'Amministratore di Sistema.

- Il Personal Computer deve essere spento al termine della propria attività lavorativa, prima di lasciare l'ufficio oppure in caso di assenza prolungata dall'ufficio stesso. Lasciare infatti un elaboratore incustodito potrebbe essere causa di utilizzo improprio da parte di terzi senza che per l'Azienda ci sia la possibilità di fornire la prova dell'indebito uso.
- Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro se non con l'espressa autorizzazione del Responsabile designato e dell'Amministratore di Sistema dell'Azienda.
- Ogni dipendente deve prestare la massima attenzione ai supporti di memorizzazione di origine esterna, avvertendo senza indugio il Responsabile designato e l'Amministratore di Sistema nel caso in cui si dovesse rilevare la presenza di virus.
- È vietato utilizzare gli strumenti informatici dell'Amministrazione al fine di custodire, far circolare ovvero promuovere, materiale pubblicitario personale, codice maligno (virus, trojan horses, programmi non licenziati) e ogni altra tipologia di materiale non autorizzato.
- È vietato copiare, scaricare ovvero mettere a disposizione di altro materiale protetto dalla legge sul diritto di autore (documenti, files musicali, film e filmati) di cui l'Azienda non abbia acquisito i diritti.
- È vietato rimuovere, danneggiare deliberatamente ovvero asportare componenti hardware.
- È fatto obbligo al dipendente in possesso di software antivirus di mantenere sempre attivo il programma con riferimento all'ultima versione disponibile. In caso di impossibilità ad operare in questo senso, è necessario fornire immediata segnalazione al Responsabile designato ed all'Amministratore di Sistema dell'Azienda.
- Il dipendente al quale sia stato assegnato dall'Amministrazione un elaboratore portatile, è responsabile dello stesso e deve custodirlo con diligenza sia durante gli spostamenti che durante l'utilizzo nel luogo di lavoro.
- Ai PC portatili si applicano le stesse regole di utilizzo previste per i PC fissi connessi in Rete.

#### **Con riferimento al collegamento ad Internet**

- È vietato l'accesso e l'utilizzo delle risorse di rete in assenza di preventiva autenticazione informatica da parte dell'Unità di Elaborazione allo scopo preposta.
- È vietato l'utilizzo di *modem/access point* per l'accesso ad Internet, salvo specifica autorizzazione in tal senso da parte del Responsabile designato e dell'Amministratore di Sistema dell'Azienda.
- Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'Azienda.
- Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento dell'attività istituzionale. È proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
- Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
- È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on line e simili salvo i casi espressamente autorizzati o attinenti ai compiti ed alle mansioni assegnate e con il rispetto delle normali procedure di acquisto.
- È vietata ogni forma di registrazione a siti o a mailing list i cui contenuti non siano legati allo svolgimento dell'attività lavorativa istituzionale.

- È vietata la partecipazione a Forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (ovvero nicknames) se non strettamente attinenti all'attività lavorativa svolta.
- È vietata tassativamente la navigazione in siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche e sindacali o le abitudini sessuali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti oltraggiosi, discriminatori ovvero che offendono il comune senso del pudore.
- Al dipendente non è consentito:
  - servirsi o dar modo ad altri di servirsi della stazione di accesso ad Internet per attività non istituzionali, per attività realizzate in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
  - scaricare software dalla rete se non espressamente autorizzato del Responsabile designato e dall'Amministratore di Sistema dell'Azienda;
  - utilizzare internet provider diversi da quello ufficiale dell'Azienda e connettere stazioni di lavoro aziendali alle reti di tali provider con sistemi di connessione diversi da quello centralizzato;
  - usare la rete in modo difforme da quanto previsto dal presente provvedimento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

#### **Con riferimento all'utilizzo dei Supporti Magnetici o Ottici**

- non è consentito scaricare files (programmi, archivi di dati, ecc) contenuti in supporti magnetici e/o ottici che non abbiano attinenza con la propria prestazione lavorativa;
- è fatto obbligo di sottoporre a controllo preventivo tutti i files di provenienza incerta o esterna, attinenti all'attività lavorativa.

#### **Con riferimento all'utilizzo della Posta Elettronica**

- L'utilizzo del servizio di posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali l'Azienda assegna una casella di posta di servizio ovvero personale e nominativa.
- La casella di posta elettronica istituzionale è uno strumento di lavoro che deve pertanto essere utilizzato esclusivamente per esigenze connesse all'attività lavorativa. Non sono ammessi utilizzi diversi o privati dell'indirizzo. I dipendenti ai quali è assegnata, sono responsabili del corretto utilizzo della stessa.
- È fatto divieto di utilizzare le caselle di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti alla propria attività svolta per l'Azienda, salvo diversa esplicita autorizzazione in tal senso.
- La casella di posta elettronica deve essere mantenuta in ordine, cancellando periodicamente i documenti inutili e gli allegati ingombranti e non deve essere utilizzata come archivio.
- È vietato utilizzare il servizio di posta elettronica istituzionale per inoltrare catene telematiche, appelli, petizioni, giochi, scherzi, barzellette, e altre e-mail che non abbiano attinenza con l'attività lavorativa. Se si riceveranno messaggi di tale tipo, si renderà necessario informare con immediatezza il Responsabile designato e l'Amministratore di Sistema dell'Azienda. In ogni caso, è fatto espresso divieto di attivare gli allegati di tali messaggi.

- È vietato utilizzare tecniche di “mail spamming”, cioè di invio massiccio di comunicazioni a liste di utenti non istituzionali. È parimenti vietato allegare al testo delle comunicazioni materiale potenzialmente insicuro (programmi, macro, scripts).

Si ribadisce che, i soggetti individuati come persone autorizzate al trattamento dei dati possono accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti ed alle funzioni istituzionali loro assegnate.

Le istruzioni saranno soggette a revisione periodica ed eventuale aggiornamento conseguente a modifiche normative o dei processi interni.

\_\_\_\_\_, addì \_\_\_\_\_

Il Dirigente, Responsabile di Struttura, designato allo svolgimento di specifici compiti e funzioni connessi al trattamento.

\_\_\_\_\_

Per ricevuta  
L'Autorizzato

\_\_\_\_\_