INFORMATIVA TRATTAMENTO DATI DEL PERSONALE DIPENDENTE

Ai sensi dell'articolo 13 del Regolamento EU 16/679 La informiamo che i Suoi dati sono trattati dalla APSP Casa di Riposo S. Vigilio – Fondazione Bonazza di Spiazzo (TN), titolare del trattamento e in particolare che:

Finalità del trattamento
Il trattamento a cui sono e saranno sottoposti i dati personali acquisiti nell'ambito della gestione del rapporto di lavoro (dati anagrafici, dati di contatto, dati identificativi, ecc.) ha le seguenti finalità:
- instaurazione e gestione del rapporto con il personale dipendente;
- adempimento di obblighi fiscali e contabili;
- applicazione della legislazione previdenziale e assistenziale;
- trattamento giuridico ed economico del personale;
- adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali;
- igiene e sicurezza del lavoro.

Trattamento di categorie particolari di dati personali e/o dati personali relativi a condanne penali e reati
Il trattamento riguarda anche le seguenti categorie particolari di dati personali e/o dati personali relativi a condanne penali e reati: contributi sindacali; permessi, congedo straordinario ed aspettative sindacali; condanne e procedimenti giudiziari pendenti contenuti in dichiarazioni sostitutive ai sensi del D.P.R. n. 445/2000.

Conferimento dei dati
I dati sono di norma raccolti presso l'interessato. Per l'instaurazione e la prosecuzione del rapporto di lavoro, nonché per la corretta quantificazione della retribuzione, è necessario il conferimento dei Suoi dati anagrafici e quelli di eventuali familiari a carico o componenti del nucleo familiare. L'eventuale non comunicazione di tali dati, comporta l'impossibilità da parte del titolare di garantire la congruità del trattamento stesso ai patti contrattuali, nonché l'impossibilità di adempiere agli obblighi imposti dalla normativa fiscale, amministrativa o del lavoro. In caso di richiesta di accredito dello stipendio presso istituti bancari, è necessario il conferimento degli estremi del c/c bancario. Per adempiere a richieste specifiche del dipendente o per obbligo di legge o contrattuale, il trattamento potrebbe riguardare anche dati idonei a rivelare lo stato di salute (assenza per malattia, maternità, infortunio, inidoneità a determinate mansioni, categorie protette), l'adesione a sindacato (assunzione di cariche sindacali, richiesta di trattenute per quote di associazione), l'adesione a partito politico (richiesta di permessi o aspettativa per cariche pubbliche elettive), convinzioni religiose (richiesta di fruizione di festività religiose), opinioni filosofiche (assolvimento di obbligo di leva quale obiettore di coscienza), origini razziali ed etniche ecc.
Il trattamento dei dati personali conferiti si basa sulla vigente normativa in materia di rapporto di lavoro, tra cui si indica: Legge n. 104/92 "legge quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate"; Legge n. 68/99 "norme per il diritto al lavoro dei disabili"; Decreto Legislativo 81/2008 "Testo Unico delle disposizioni legislative in materia di tutela della salute e della sicurezza nei luoghi di lavoro"; Decreto legislativo 38/00 "Disposizioni in materia di assicurazione contro gli infortuni sul lavoro e le malattie professionali"; Decreto Legislativo 151/01 " Testo unico delle disposizioni legislative in materia di tutela e sostegno della maternità e della paternità"; Decreto Legislativo 215/03 "Attuazione della Direttiva 2000/43 CE per la parità di trattamento delle persone indipendentemente dalla razza e dalla origine etnica"; Decreto Legislativo 216/03 "Attuazione della Direttiva 2000/78 CE per la parità di trattamento in materia di occupazione e condizioni di lavoro"; Legge 300/70 "Statuto dei lavoratori"; Decreto Legislativo 165/01 "Norme Generali sull'ordinamento del lavoro alle dipendenze delle Amministrazioni Pubbliche"; TU 81/2008; C.C.P.L; L.R. 21/09/2005 n. 7; Regolamento organico del personale dipendente; L.P. n.14/91; L.P. n.6/98; Statuto dell'Ente.
Altre disposizioni normative possono essere richiamate nella documentazione consegnata all'interessato in sede di assunzione o, se del caso, in momenti successivi. Eventuali variazioni di dati dovranno essere tempestivamente comunicate al titolare del trattamento.

Base giuridica del trattamento
La base giuridica del trattamento dei dati raccolti è rappresentata dalla necessità di dare esecuzione ad un obbligo di legge e/o eseguire un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Modalità del trattamento
I dati vengono trattati nel rispetto delle misure di sicurezza tecniche e organizzative previste dal Regolamento UE attraverso procedure adeguate a garantire a riservatezza degli stessi. I dati non saranno trattati mediante processi decisionali automatizzati. Tutti i dati conferiti sono trattati secondo i principi di correttezza, liceità e trasparenza sia

WHITE LIST: elenco di siti che il datore di lavoro ritiene comunemente attinenti all'attività lavorativa svolta.
BLACK LIST: elenco di siti che presentano contenuti non attinenti all'attività lavorativa e, per questa ragione, sottoposti a filtri che si attivano qualora l'utente cerchi di accedervi.
TITOLARE DEL TRATTAMENTO: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4 Reg UE 16/679).
INCARICATO: persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di trattamento di dati personali.
DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 Reg UE 16/679).

2. UTILIZZO DELLA RETE E DEL PERSONAL COMPUTER

2.1. L'utilizzo di tutti gli strumenti informatici di proprietà del titolare deve avvenire osservando regole di buona diligenza e prudenza, con senso di responsabilità e seguendo le istruzioni impartite dal titolare e dalle persone delegate.
2.2. L'uso degli strumenti informatici aziendali (PC, attrezzatura informatica, notebook, accesso alla rete internet, telefoni mobili, ecc.) è consentito unicamente agli utenti autorizzati mediante attribuzione di apposito incarico al trattamento. Ogni utilizzo dei predetti beni non inerente all'attività lavorativa è tassativamente vietato.
2.3. Le unità di rete sono aree di condivisione di dati ed informazioni strettamente legati all'attività lavorativa. I file ivi dislocati devono avere attinenza con le attività svolte da ciascun incaricato e qualunque file che non sia legato all'attività lavorativa non può essere ivi dislocato, nemmeno per brevi periodi. Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi.
2.4 Ogni utente è responsabile per l'uso riferito al proprio account ed è personalmente tenuto a conformarsi a modalità di utilizzo atte ad impedire accessi da parte di terzi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.
2.5. Le disposizioni di seguito riportate, relative alle credenziali di autenticazione, contribuiranno a garantire la sicurezza nell'accesso:
a) scegliere una password composta da almeno 8 caratteri alfanumerici che non contenga riferimenti che riconducano agevolmente all'incaricato;
b) la stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il blocco del computer;
c) la password è personale, riservata e non può essere ceduta o comunicata ad alcuno. E' pertanto vietato l'uso della password di altri utenti;
d) è obbligatorio modificare la password ogni volta che il sistema ne faccia richiesta o almeno regolarmente ogni tre/sei mesi (trattamento dati sensibili/comuni);
e) per esigenze operative o di sicurezza e integrità del sistema e dei dati, il titolare, tramite l'Amministratore di sistema ha facoltà di modificare la password degli utenti;
f) qualsiasi attività svolta utilizzando un codice utente e la relativa password sarà ricondotta nella sfera di responsabilità dell'utente assegnatario del codice. L'utente è civilmente responsabile di ogni danno cagionato al titolare, all'Internet Provider e/o a terzi, non solo in relazione ai propri fatti illeciti ma anche per quelli commessi da chiunque utilizzi il suo codice utente e password;
2.6. Per evitare il pericolo di introdurre virus informatici o di alterare la stabilità delle applicazioni è vietato scaricare ed installare programmi, salva espressa autorizzazione da parte del titolare o dell'Amministratore di sistema.
2.7. Non è consentito modificare le configurazioni del proprio PC. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.
2.8. Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.
2.9. Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema causati da comportamento doloso o comunque non conforme alle istruzioni e disposizioni, deve darne immediata comunicazione al titolare o all'Amministratore di Sistema. Salvo preventiva espressa autorizzazione non è consentito eseguire operazioni di manutenzione ordinaria o straordinaria autonomamente.
2.10 Non è consentito archiviare sul proprio pc, sul server o su qualunque altra area condivisa, file e dati non inerenti alla propria attività lavorativa.
2.11 E' vietato l'uso masterizzatori o altri supporti di registrazione di dati (ad es. dischi fissi esterni, chiavette USB, ecc.) per registrare dati salvi i casi direttamente autorizzati.
2.12 Il titolare del trattamento si riserva la facoltà di procedere alla rimozione di ogni applicazione o file ritenuti pericolosi per la sicurezza del sistema, non attinenti all'attività lavorativa o acquisiti ed installati in violazione del presente disciplinare, sia sui PC degli incaricati sia sulle unità di rete.
2.13 L'utente è tenuto alla periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili o duplicati onde evitare un'archiviazione ridondante.
2.14 L'utente deve limitare le stampe dei dati solo a quelle strettamente necessarie, ritirandole prontamente dai vassoi delle stampanti comuni.
2.15 E' fatto divieto di accedere contemporaneamente con lo stesso account da più PC.

2.16 Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferire con la connettività altrui o con il funzionamento del sistema e quindi di: utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti, utilizzare software rivolti alla violazione della sicurezza del sistema e della privacy; sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate; modificare le configurazioni impostate dall'amministratore di sistema; limitare o negare l'accesso al sistema a utenti legittimi; effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc.); distruggere o alterare dati altrui; collegare in rete personal computer non di proprietà del titolare.

3. UTILIZZO DI PC PORTATILI

3.1 L'utente al quale venga assegnato un computer portatile ne è responsabile e dovrà custodirlo con la dovuta diligenza sia durante l'utilizzo nel luogo di lavoro.
3.2 In caso di utilizzo all'esterno del luogo di lavoro, i notebook dovranno essere custoditi con attenzione e conservati in luogo sicuro. PC portatili e Tablet potrebbero essere dotati della funzione di localizzazione geografica. Tale funzionalità deve essere disattivata dall'utente.
3.3 Al computer portatile si applicano le regole sopra indicate per i PC connessi in rete, con particolare attenzione alle disposizioni concernenti i profili di accesso (password).
3.4 Sull'hard disk devono essere conservati solo i file strettamente necessari all'attività lavorativa, rimuovendo comunque, prima della restituzione, quelli elaborati ed ivi salvati.
3.5 E' necessario collegarsi periodicamente e, almeno, con cadenza settimanale, alla rete interna per consentire gli aggiornamenti dell'antivirus, del sistema operativo, nonché la sincronizzazione della posta elettronica e relative cartelle pubbliche.
3.6 E' fatto divieto di utilizzare abbonamenti Internet privati per collegarsi alla rete.

4. UTILIZZO DELLA RETE INTERNET

4.1 L'accesso alla rete Internet può essere effettuato da qualsiasi utente che sia autenticato (credenziali di accesso) su una qualsiasi postazione di lavoro connessa. Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
4.2 Il lavoratore deve ricordare che Internet è uno strumento di lavoro e quindi che è possibile che il datore di lavoro, per ridurre i casi di utilizzo improprio (es: visione di siti non correlati all'attività lavorativa, download di file e software, uso della rete per finalità completamente estranee alla propria mansione, ecc.), adotti misure atte ad evitare l'esercizio di un controllo a posteriori dei lavoratori. Fra queste misure si possono enumerare l'individuazione di white list (composte da soli siti istituzionali, rispetto ai quali la navigazione è correlata e funzionale allo svolgimento della prestazione lavorativa) o black list (composte da tutti quei siti che, oltre a non avere attinenza con il lavoro, presentano contenuti non in linea con le politiche di gestione adottate dal titolare) ovvero tramite l'impostazione di filtri sul firewall (soluzione adottata dal titolare).
4.3 E' vietato il download di software gratuiti (freeware) e shareware nonché di file video o musicali prelevati da siti Internet, salvi i casi direttamente autorizzati dal titolare.
4.4 E' vietata ogni forma di registrazione a siti, newsletter, blog e quant'altro assimilabile, salvi i casi direttamente autorizzati. È vietata la partecipazione a forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) salvi i casi direttamente autorizzati.
4.5 È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvi i casi direttamente autorizzati.
4.6 Non è consentito accedere ed utilizzare la rete internet in modo difforme da quanto previsto dal presente disciplinare e, ovviamente, dalle leggi penali, civili ed amministrative in materia. In ogni caso, ogni utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei siti ai quali accede, delle informazioni che immette e riceve.
4.7 Qualora un utente dovesse riscontrare malfunzionamenti, guasti o situazioni di rischio per la sicurezza o l'integrità del sistema causati da comportamento doloso o comunque non conforme alle istruzioni e disposizioni è tenuto a darne immediata comunicazione al titolare.
4.8 Gli eventuali controlli, compiuti dal titolare per il tramite di personale incaricato, potranno avvenire mediante un sistema di analisi dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre un mese, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del titolare.

5. UTILIZZO DELLA POSTA ELETTRONICA

5.1 Il sistema di posta elettronica attivato sulla rete della società è da intendersi quale strumento di lavoro e come tale deve essere utilizzato.
5.2 Può essere assegnato un account di posta elettronica ad ogni utente della rete informatica o indirizzi condivisi tra più utenti.
5.3 L'accesso al sistema di posta elettronica è protetto dalla richiesta di autenticazione.
5.4 Le disposizioni di seguito riportate sono enucleate al fine di garantire un corretto utilizzo della strumento di posta elettronica:
a) all'utente non è consentito servirsi dell'account fornito dal titolare per l'invio di mail non connesse con l'attività e la mansione svolta (es: mail a contenuto privato, giochi, appelli, petizioni, catene di S. Antonio, ecc.);
b) si deve evitare di allegare al testo delle comunicazioni materiale potenzialmente insicuro o file di dimensioni eccessive. In quest'ultimo caso si dovranno utilizzare formati compressi (zip, rar, ecc.);
c) nel caso di mittenti sconosciuti o di messaggi dall'oggetto insolito, è consigliata l'eliminazione senza l'apertura del messaggio. Lo stesso vale nel caso di messaggi provenienti da mittenti conosciuti che tuttavia presentano allegati con

particolari estensioni (es: .exe, .scr, .pif., .bat..);
d) nel caso in cui si debba inviare un documento all'esterno, è preferibile utilizzare un formato protetto da scrittura (es: Acrobat);
e) si deve evitare l'invio di mail che contengano categorie particolari di dati personali; qualora ciò sia necessario per determinate esigenze, questi devono essere inviati comunicando al richiedente un codice identificativo per ogni soggetto e trasmettendo separatamente il documento privo del nominativo dell'interessato e crittografando i file con password che dovrà essere comunicata al destinatario del messaggio per altro mezzo;
f) qualora il messaggio debba essere inviato a più soggetti, gli indirizzi vanno inseriti solo nel campo "CCn" per tutelare la riservatezza dei medesimi, che ricevono il messaggio conoscendo solamente il mittente;
g) prevedere, in caso di assenza prolungata del lavoratore (es: ferie), l'invio di messaggi di risposta automatica che indichino la durata dell'assenza ed il nominativo del soggetto al quale è possibile rivolgersi;
h) l'iscrizione a mailing list o newsletter è concessa solo per motivi strettamente professionali: prima di iscriversi è necessario verificare l'affidabilità ed ottenere l'autorizzazione del titolare;
i) l'intestatario dell'account ha facoltà di delegare ad altri il diritto d'accesso allo strumento in caso di assenza prolungata ai fini di garantire la continuità nell'attività lavorativa. Il fiduciario dovrà essere scelto e nominato fra i colleghi e, qualora dovesse accedere alla casella di posta della persona assente, non potrà comunque considerare i messaggi che presentino contenuto non attinente alle motivazioni per cui si effettua l'accesso.
l) il titolare, l'Amministratore di sistema o chi da essi incaricato può avere accesso all'account a seguito del riscontro di situazioni che abbiano pregiudicato il funzionamento del sistema.
5.5 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
5.6 I documenti inerenti il know how aziendale tecnico o commerciale protetto non possono essere comunicati all'esterno senza la preventiva autorizzazione del titolare.

6. PROTEZIONE ANTIVIRUS
6.1 L'utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico del titolare mediante virus o mediante ogni altro software aggressivo.
6.2. Qualora il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
a) sospendere ogni elaborazione in corso senza spegnere il computer;
b) segnalare l'accaduto all'amministratore di sistema.
6.3. Non è consentito l'utilizzo di cd/dvd rom, cd/dvd rescrivibili, nastri magnetici, chiavette per porte USB di provenienza ignota.
6.4. In caso di utilizzo autorizzato dei suddetti dispositivi, si dovrà procedere alla verifica degli stessi e nel caso in cui vengano rilevate anomalie alla loro consegna all'amministratore di sistema.

7. INTERRUZIONE D'UFFICIO DEL SERVIZIO
7.1 Il titolare si riserva di sospendere temporaneamente il servizio di accesso ad Internet e alla posta elettronica nei seguenti casi:
a) qualora venga meno la condizione di dipendente o collaboratore;
b) qualora si accerti un uso non corretto del servizio e degli strumenti informatici messi a disposizione;
c) in caso di manomissioni e/o interventi impropri su hardware/software;
d) in caso di diffusione o di comunicazione imputabile direttamente o indirettamente all'utente relativamente a profili d'accesso o altre informazioni tecniche riservate;
e) accesso a directory/file/siti non rientranti fra quelli per cui l'utente abbia autorizzazione.

8.UTILIZZO DEL TELEFONO
8.1 Il telefono è uno strumento di lavoro e come tale deve esser utilizzato. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.
8.2. Eventuali telefonate a carattere privato potranno essere effettuate con moderazione ed in casi di necessità.
8.3 I cellulari e gli smartphone affidati agli utenti per rendere la prestazione lavorativa sono strumenti di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa. Gli utenti cui è assegnato un cellulare o uno smartphone aziendale sono responsabili del suo utilizzo e della sua custodia. Al cellulare aziendale e allo smartphone si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare o dello smartphone messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.
8.4 I cellulari e gli smartphone potrebbero essere dotati della funzionalità di localizzazione geografica. Tale funzione deve essere disattivata dall'utente. E' vietato effettuare il Jailbreak del dispositivo e più in generale è vietata qualsiasi procedura di sblocco del device aziendale assegnato, ad esempio, per installare/utilizzare applicazioni non autorizzate.

9. CONTROLLI E SANZIONI DISCIPLINARI
9.1. Sono interdetti al datore di lavoro controlli del personale dipendente effettuati in maniera diretta, prolungata, costante o indiscriminata (art. 4, Statuto dei lavoratori, l. 300/1970). Ciò premesso, oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo diretto dell'attività lavorativa, è facoltà del titolare tramite gli addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.
9.2. Il titolare può avvalersi di sistemi controllo relativi al corretto utilizzo degli strumenti informatici messi a disposizione

dei propri collaboratori e dipendenti che consentano indirettamente un controllo a distanza sull'effettivo adempimento della prestazione lavorativa: tali controlli saranno effettuati qualora le misure minime preventivamente esposte non siano state sufficienti per evitare comportamenti anomali.
9.3. I controlli saranno svolti con gradualità, secondo i principi di pertinenza e non eccedenza. In seguito si espongono le modalità di esercizio di tali controlli: in prima battuta si effettuerà un controllo preliminare su dati anonimi ed aggregati; si procederà pertanto con verifiche di ufficio o gruppo di lavoro, in modo da individuare l'area da richiamare all'osservanza delle regole prestabilite.
Il controllo anonimo può dare atto ad un avviso di rilevazione di un utilizzo inadeguato degli strumenti aziendali; contestualmente si diramerà una nota di richiamo invitando tutti i dipendenti e collaboratori ad attenersi ai compiti e alle mansioni impartite tenuto conto del dovere di conformarsi alle presenti regole.
Se si dovesse ripetere l'anomalia sarà facoltà della società procedere con controlli mirati, anche su base individuale, e successivamente, in caso di infrazioni, adottare sanzioni disciplinari.
9.4. L'adozione delle sanzioni disciplinari avverrà a norma dell'art. 2106 c.c. del codice civile, dell'art. 7 dello statuto dei lavoratori (legge 300/1970), del contratto di riferimento e del relativo codice disciplinare vigente.
9.5. I dati contenuti nei file di log, relativi agli accessi ad Internet e al traffico telematico, possono essere conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza. I file di log potranno essere utilizzati in tali casi:
a) produzione di report statistici che presentino i dati relativi alla navigazione in forma aggregata e anonima;
b) per l'analisi dei problemi riscontrati nel sistema e soluzione dei medesimi, estraendo i dati in modo aggregato e in forma anonima.

10. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY
10.1 Oltre al rispetto del presente regolamento è fatto obbligo di attenersi scrupolosamente alle disposizioni in materia di trattamento dati personali e alle relative misure di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento e nel materiale formativo messo a disposizione di ciascun collaboratore e dipendente osservando con attenzione le prescrizioni del Reg. UE 16/679.
Ciascun incaricato assume la piena responsabilità nel merito dell'osservanza del modello organizzativo, delle misure di sicurezza, delle indicazioni fornite dall'amministratore di sistema o dal responsabile per la protezione dei dati, se designato.
Ciascun incaricato è tenuto a mantenere un costante flusso informativo con il responsabile per la protezione dei dati personali, segnalando a quest'ultimo ogni eventuale criticità o violazione sul sistema di sicurezza adottato.

11. AGGIORNAMENTO E REVISIONE DEL DISCIPLINARE INTERNO
11.1 Il presente Regolamento è soggetto a verifica con eventuali revisioni ed aggiornamenti con periodicità annuale e, comunque, in caso di modifiche e/o integrazioni della normativa di legge.
11.2 Al presente disciplinare interno viene data pubblicità mediante affissione in bacheca anche ai sensi e per gli effetti dell'art. 7 legge 10 maggio 1970 n. 300 in relazione al codice disciplinare del quale costituisce parte integrante.

Spiazzo, 18/10/2018

IL TITOLARE DEL TRATTAMENTO
APSP Casa di Riposo S. Vigilio – Fondazione Bonazza

IL PRESIDENTE