AZIENDA SANITARIA PROVINCIALE

Servizio Sanitario Nazionale – Regione Sicilia
AZIENDA SANITARIA PROVINCIALE AGRIGENTO
Direzione Generale- Ufficio Protezione Dati
Tel 0922/407232- mail:ufficio.protezionedeidati@aspag.it
Viale Della Vittoria n. 321, Agrigento 92100
Web: www.aspag.it

Procedura interna

PER L'UTILIZZO DELLA DOTAZIONE INFORMATICA, DELLA POSTA ELETTRONICA, INTERNET E PER LA TUTELA DEI SISTEMI INFORMATICI.

INDICE

1. Premessa

La presente Procedura interna definisce principi e regole comportamentali di buona condotta a cui tutti i dipendenti e collaboratori (compresi fornitori esterni, consulenti e *partner*) che operano per l'Azienda Sanitaria Provinciale di Agrigento (di seguito anche "ASP Agrigento") devono uniformarsi, per fare fronte alle esigenze di sicurezza nel trattamento dei dati personali e per minimizzare il rischio di violazione dei dati (data breach), nel rispetto del Regolamento UE 2016/679.

Ai fini di questa procedura si specifica che con il termine **"dati"** deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore (a prescindere dal rapporto contrattuale con l' Azienda) può venire a conoscenza e delle quali deve garantire la riservatezza e la segretezza.

Anche fra colleghi oppure fra dipendenti e collaboratori esterni è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

2. Riferimenti normativi

la presente procedura è adottata in conformità:

- al Regolamento Generale sulla Protezione dei Dati (GDPR) UE n.679/2016;

- al D.Lgs 30 giugno 2003 n.196 "Codice in materia di protezione dei dati personali" come modificato e integrato dal D.Lgs n. 101/2018;

- Provvedimento del Garante per la protezione dei dati personali " Linee guida per posta elettronica e Internet" de! 1° marzo 2007;

- Provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema- del 27 novembre 2008;

- Provvedimento del Garante "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per ii loro adempimento" del 25 giugno 2009;

3. Campo di applicazione

La presente Procedura interna si applica a tutto il personale dipendente e ai collaboratori di ASP Agrigento che, nello svolgimento delle proprie mansioni lavorative, impiegano le risorse informatiche di proprietà dell'ASP Agrigento.

Ai fini dell'applicazione della presente Procedura, per risorsa informatica si intende:

- la dotazione informatica affidata al personale dipendente e a collaboratori, comprensiva di *personal computer desktop* o portatili, *smartphone*, *tablet*, ecc.;
- l'accesso alle risorse di rete Internet e Intranet;
- l'accesso e l'utilizzo della posta elettronica aziendale.

4. Regole di condotta generali

Gli utenti assegnatari sono direttamente responsabili dei dispositivi informatici loro affidati e, più in generale, delle risorse informatiche da essi accedute.

Tali dispositivi devono essere impiegati esclusivamente per finalità professionali legate allo svolgimento delle mansioni correlate all'incarico ricevuto da parte di ASP Agrigento.

Salvo apposita ed esplicita autorizzazione da parte del proprio Responsabile di Struttura e, qualora autorizzato l'utilizzo, esclusivamente secondo le modalità previste dal presente Procedura interna, non è consentito l'uso di dispositivi personali (PC *desktop, laptop, pen-drive, hard disk* esterni, CD/DVD, ecc.) per memorizzare e trattare dati aziendali.

È in ogni caso vietato l'accesso e l'utilizzo di reti anonime aperte (come, ad esempio, Wi-Fi pubblici aperti).

Quando l'utente visualizza informazioni riservate su uno schermo, deve verificare che nell'ambiente circostante non siano presenti altri soggetti a cui non sia consentita (o non risulti opportuna) la visualizzazione di tali informazioni, specialmente se di carattere confidenziale.

Nel caso in cui tale condizione di riservatezza non fosse garantita, è necessario attendere che le persone non autorizzate alla visione delle informazioni si allontanino; in alternativa, l'utente assegnatario dovrà spostarsi direttamente in altro luogo e procedere con l'attività lavorativa.

In caso di allontanamento dalla propria postazione di lavoro e, dunque, dal dispositivo informatico, l'utilizzatore deve provvedere ad attivare il salvaschermo protetto da *password* senza attenderne l'attivazione automatica, allo scopo di impedire l'accesso alle informazioni a soggetti non autorizzati.

Particolare attenzione va posta durante l'inserimento dei codici di accesso (*username* e *password*).

Gli utenti, prima di digitare sulla tastiera i codici di accesso, devono assicurarsi che nessuno possa prenderne visione.

L'utente provvede a modificare immediatamente le proprie credenziali nell'ipotesi in cui soggetti terzi o altri utenti possano essere venuti a conoscenza delle sue credenziali in maniera non autorizzata.

Username e *password* non devono mai essere condivisi con alcuno

5. Prescrizioni sull'utilizzo di stampanti e fotocopiatori

Tutti i documenti devono essere immediatamente recuperati dalle stampanti, dai fax e dalle fotocopiatrici, specialmente quelle di rete, in particolare gli utenti devono:

- Stampare documenti solo se strettamente necessari per lo svolgimento dell'attivita lavorativa;

- utilizzare le stampanti di rete in luogo di quelle locali per ridurre i materiali di consumo;
- spegnere le stampanti in caso di inutilizzo ed a fine giornata lavorativa;
- in caso di stampante condivisa, qualora possibile, attivare la funzione che genera un PIN da digitare sulla stampante per sbloccare la stampa al momento del ritiro. In ogni caso, evitare di lasciare le stampe incustodite e ritirare immediatamente le copie non appena stampate, in modo che non possano venirne a conoscenza persone non autorizzate.

6. Prescrizioni sull'utilizzo di supporti rimovibili

I supporti rimovibili sono quei dispositivi che consentono di copiare o archiviare dati, files, documenti esternamente al computer (CD-ROM, DVD, penne o chiavette USB, hard disk portatili, ecc.).

L'uso di supporti di memorizzazione rimovibili è vietato.

Qualora il loro utilizzo si renda assolutamente necessario, l'Utente è tenuto ad adottare le seguenti cautele:

- utilizzare i dispositivi rimovibili aziendali esclusivamente su computer aziendali;
- prima dell'uso, sottoporre sempre tutti i supporti di origine estema a scansione antivirus/antimalware con un programma antivirale aggiomato ed avvertire immediatamente l'Amministratore di sistema del rilevamento di virus o malware di qualsiasi natura;
- qualora vi sia l'assoluta necessità di memorizzare su dispositivi rimovibili dati particolari, l'Utente è tenuto ad adottare sistemi di crittografia, avendo cura di permettere la lettura solo agli aventi diritto, ovvero, in mancanza, utilizzare sistemi di pseudonimizzazione (ad esempio, contrassegnando i documenti semplicemente con un codice) o sistemi di anonimizzazione;
- custodire con cura i supporti rimovibili su cui sono memorizzati dati personali in armadi chiusi a chiave, al fine di evitare che il contenuto possa essere trafugato, o alterato, e/o distrutto, ovvero conosciuto da terzi non autorizzati ad accedervi;
- procedere alla cancellazione "sicura" dei dati personali presenti sui supporti magnetici od ottici, prima del loro riutilizzo;
- consegnare i supporti magnetici obsoleti (dischetti, nastri, chiavi USB, CD riscrivibili ed altro) all'Amministratore di sistema per l' opportuna distruzione, onde evitare che il loro contenuto possa essere recuperato successivamente alla cancellazione.

7. Prescrizioni in materia di sicurezza privacy per lo smart working /lavoro agile

L' Azienda può mettere a disposizione degli Utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna.

Anche in tal caso l'Utente (ad es. smart-worker) è tenuto a conformarsi a tutte le prescrizioni di sicurezza dettate nella presente procedura, per quanto compatibili.

L' Amministratore di Sistema è tenuto al controllo della sicurezza delle postazioni esterne remote, negando o interrompendo l'accesso alla rete agli Utenti che utilizzino dispositivi non adeguatamente protetti e/o aggiomati che possano costituire una concreta minaccia per la sicurezza

informatica dell'Azienda.

8. Gestione della rete informatica interna e della rete internet

L'utilizzo di Internet e la navigazione in rete è consentita ai titolari di *account* espressamente autorizzati.

Le credenziali, pur se assegnate personalmente, sono da considerarsi di proprietà aziendale poiché costituiscono semplicemente uno strumento di lavoro messo a disposizione dall'ASP Agrigento per svolgere le attività legate alle mansioni assegnate.

L'accesso ad Internet è fornito allo scopo di consentire il reperimento di eventuali informazioni necessarie allo svolgimento dell'attività lavorativa.

Essendo uno strumento di lavoro, i soggetti cui l'ASP Agrigento consente l'accesso a Internet sono responsabili del corretto utilizzo nel pieno rispetto della normativa di riferimento vigente (Regolamento Europeo 2016/679), nonché secondo normali *standard* di correttezza, buona fede e diligenza professionale, avendo cura di non tenere comportamenti che possono comportare rischi per l'integrità, la riservatezza e la disponibilità delle informazioni aziendali.

L'Azienda, con il presente documento, ha inteso definire per gli utenti uno specifico codice di condotta in modo da evitare comportamenti che inconsapevolmente potrebbero, attraverso l'uso improprio, danneggiarla.

In particolare, è assolutamente vietato:

- accedere alla rete con un codice d'identificazione di un altro operatore;
- condividere cartelle in rete sprovviste di password, fatte salve situazioni particolari da autorizzare caso per caso;
- alterare la configurazione di rete di stazioni di lavoro e di altri dispositivi in rete (stampanti condivise, ecc...);
- aggiungere protocolli di rete o servizi in rete (per es. condivisione di stampanti in
- rete, browsing di risorse di rete, ecc.);
- scaricare, copiare, distribuire documenti o altro, in violazione delle leggi sul diritto di autore;
- effettuare installazioni non autorizzate di modem per linee analogiche o digitali per l'accesso a banche dati esterne o interne all'Azienda;
- effettuare installazioni di hardware o software di qualsiasi tipo che consenta o faciliti il superamento delle misure di sicurezza adottate;
- nel caso in cui il software antimalware rilevi la presenza di un virus/malware, sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto all'Amministratore di sistema ed al Dirigente Informatico.

Al fine di evitare all'Utente la navigazione in siti non pertinenti l'attività lavorativa, si rende noto che è previsto l'uso di un sistema di blocco o filtro automatico che prevenga determinate operazioni, quali l'upload e l'accesso a determinati siti inseriti in una black list.

L'efficacia del sistema di filtraggio è controllata dall' Amministratore di sistema o dal Referente Informatico.

9. Assegnazione degli account

Le credenziali di autenticazione sono composte da un codice identificativo personale (*username* o *user id*) e da una parola chiave (*password*).

Lo *username* è attribuito e gestito dal personale competente di ASP Agrigento che crea una singola utenza digitale per ogni persona. Tale utenza digitale servirà per identificare univocamente ogni utente che accede alle risorse ed alle applicazioni informatiche aziendali. La *password* viene assegnata dal personale competente di ASP Agrigento e deve essere immediatamente cambiata dall'utente al primo accesso.

Devono essere rispettate specifiche regole per la *definizione*, la *custodia* ed il *cambiamento* della *password*.

Regole per la definizione della *password*:

- deve essere di lunghezza non inferiore ad 8 caratteri e preferibilmente composta da caratteri alfanumerici, maiuscoli e minuscoli, numeri e caratteri speciali;
- deve essere diversa dalle ultime 6 versioni precedentemente utilizzate;
- non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti;
- non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti o più di due caratteri posizionati in maniera contigua sulla tastiera.

Regole per custodire la *password*:

- deve essere nota esclusivamente all'utente e non può essere assegnata e/o comunicata ad altri utenti, sia interni e sia esterni;
- per l'acceso alle applicazioni aziendali non deve essere impiegata la stessa *password* utilizzata per l'accesso a servizi acceduti a titolo personale ovvero a sistemi gestiti da altre organizzazioni;
- non deve essere scritta su carta o su *post-it* visibili sulla scrivania o applicati altrove;
- non deve essere memorizzata in funzioni di *login* automatico o nel *browser* utilizzato per la navigazione Internet.

Regole per cambiare la *password*:

- deve essere obbligatoriamente cambiata dopo il primo utilizzo e successivamente almeno ogni 60 giorni;
- deve essere cambiata immediatamente nei seguenti casi:
    - nel caso in cui l'utente dovesse sospettare che altri utenti o soggetti terzi siano venuti a conoscenza della sua *password*;
    - dopo aver effettuato l'accesso ai sistemi informativi Aziendali da remoto, in particolare attraverso un PC "pubblico" o condiviso (es. Internet Cafè).

La *password* può essere annullata e sostituita con una nuova prima della scadenza, da parte del personale competente, per motivate necessità e previa informazione all'utente. In tal caso la *password* dovrà essere nuovamente modificata da parte dell'utente al primo accesso.
Tutti i possessori di utenza e *password* sono responsabili di eventuali manomissioni, utilizzi impropri o divulgazioni non autorizzate, incorrendo così nelle sanzioni disciplinari/legali applicabili.

10. Gestione della Posta Elettronica

II servizio di Posta elettronica è fomito in funzione della comunicazione dell'Azienda e delle altre attivita strumentali correlate ai fini istituzionali.

La casella di posta assegnata all'*Utente è* uno strumento di lavoro messo a disposizione per lo svolgimento della prestazione lavorativa**.**

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
L'account di posta elettronica (usemame, password ed indirizzo di posta) è fomito, insieme ad un limitato spazio disco, alle seguenti categorie di Utenti:

1) Organi, Strutture ed articolazioni aziendali centrali e periferiche (PP.OO. OO.SS.SS.) Aree di gestione, Uffici di Staff; in questo caso il formato dell'indirizzo di posta sarà: **nomeservizio@aspag.it**
2) Personale dipendente in servizio attivo; in questo caso il formato dell'indirizzo di posta sarà: nome.cognome@aspag.it;

L'attivazione dell'account avverrà su richiesta scritta autorizzata dal Dirigente responsabile della Struttura e/o Ufficio, dopo la verifica dei requisiti richiesti.
L'Utente si impegna ad adoperarsi attivamente per salvaguardare la riservatezza della sua password ed a segnalare qualunque situazione che possa inficiarla.

L'Utente sarà responsabile dell'attività espletata tramite il suo account.

La "personalizzazione" dell'indirizzo non comporta il suo carattere "privato", in quanto trattasi di strumenti di esclusiva proprietà aziendale messi a disposizione dell'Utente al solo fine dello svolgimento delle proprie mansioni lavorative.
L' Azienda si impegna ad utilizzare i dati forniti dall'Utente ai fini dell'erogazione e gestione del servizio e di attuare quanto in suo potere per proteggere la privacy dell'Utente medesimo.

L'Azienda si impegna a fornire il servizio in modo continuativo, fatte salve eventuali sospensioni dovute all'ordinaria o straordinaria manutenzione, a malfunzionamenti e ad altre eventualità.

Inoltre, l'Azienda si impegna ad effettuare regolari backup generali sui server gestiti direttamente; non sono previsti backup e ripristini individuali.

L' Azienda attuerà tutte le misure ritenute necessarie e sufficienti a minimizzare il rischio di perdita d'informazioni; ciò nonostante l'Utente solleva l' Azienda da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, al mancato invio/ricezione o all'omessa conservazione di messaggi di posta (e-mail) imputabili ad un uso inappropriato del servizio, mentre le responsabilità derivanti da guasti e/o malfunzionamenti degli apparati di gestione del software sono regolate dal contratto di affidamento Servizio come per Legge.

L' Azienda persegue la riservatezza e l'integrità dei messaggi durante il loro transito e la loro permanenza nel sistema di posta.

11. Doveri, divieti, limiti di utilizzo, responsabilità dell'utente

L'Utente si impegna, nei confronti dell'Azienda, a presidiare quotidianamente la propria casella elettronica, con l'apertura e lettura dei messaggi di posta, corrispondendo alla richiesta di avviso di recapito e monitorando costantemente le sue dimensioni per non superare il limite di spazio previsto.

L'Utente si impegna a non utilizzare il servizio per scopi illegali o non conformi alla presente procedura che comunque possano recar danno o pregiudizio all'Azienda medesima o a terzi.

L'Utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio; esonera contestualmente I'Azienda da ogni pretesa o azione che dovesse essere rivolta all'Azienda medesima da qualunque soggetto, in conseguenza di tale uso improprio del servizio.

L'Utente, inoltre, non può utilizzare il servizio in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l'utilizzo da parte di altri utenti.

L'Utente, salvo giustificabili eccezioni, di cui comunque risponde personalmente, non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino a:

- pubblicità non istituzionale, manifesta o occulta;
- comunicazioni commerciali private;
- materiale che violi la normativa vigente sulla protezione dei dati personali;
- contenuti o materiali che violino i diritti di proprieta di terzi;
- altri contenuti illegali.

In nessun caso l'Utente potrà utilizzare la posta elettronica per diffondere codici dannosi per i computer quali virus e simili.

L'Utente non può tentare di accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti.

L' utente si impegna a fare attenzione alle mail ingannevoli, controllando i file allegati di posta elettronica prima del loro utilizzo; deve evitare di aprire gli allegati e di cliccare i link contenuti in messaggi di mittenti sconosciuti, notificando l'accaduto all'Amministratore di sistema o al Referente informatico e cancellando tali mail.

Per l'invio a destinatari esterni di messaggi contenenti allegati relativi a dati personali particolari o giudiziari, l'Utente è tenuto a renderli preventivamente illeggibili, criptandoli con apposito software e comunicando al destinatario la password di cifratura attraverso un canale

diverso dalla mail (ad esempio per lettera o per telefono).

L'Utente, infine, si impegna a non divulgare messaggi di natura ripetitiva (catene di varia denominazione) anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus).

Di fronte a quest'ultima evenienza l'Utente dovrà limitarsi ad inoltrare un messaggio all'Amministratore di sistema o al dirigente Informatico.

L'Azienda si riserva la facoltà di segnalare alle Autorità competenti, per gli accertamenti ed i provvedimenti del caso, le eventuali violazioni alle presenti condizioni di utilizzo.

12. Accesso ai dati trattati dall'utente

L' Azienda, nel rispetto della normativa vigente sulla protezione dei dati, si riserva il diritto di accedere alla risorsa informatica in dotazione dell'Utente ed ai documenti in essa contenuti, per esigenze organizzative e produttive (attività di gestione, controllo, aggiomamenti ai fini della sicurezza del sistema e della rete), per la sicurezza del lavoro e per la tutela del patrimonio, nella considerazione che ogni dato trattato per mezzo degli strumenti e delle risorse informatiche appartenenti all' Azienda sarà considerato di natura aziendale e non riservata.
Le informazioni raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento.

13. Assistenza Tecnica

Le attività di manutenzione, gestione ed implementazione sono eseguite da personale intemo (con funzioni di supporto e di vigilanza sulla corretta osservanza delle prescrizioni contenute in questa procedura) e da personale afferente all'organizzazione di soggetti esterni previamente nominati dal Titolare quali Responsabili esterni, secondo le prescrizioni contenute nel Provvedimento del Garante del 2008, cui si fa rinvio.

A seguito di chiamata dell'Utente o in caso di necessità per la rilevazione tecnica di problemi nel sistema informatico, l'Amministratore di sistema ed il suddetto personale incaricato sono autorizzati a compiere interventi nel sistema informatico aziendale per risolvere problemi tecnici e/o manutentivi, nonchè per garantire la sicurezza e la salvaguardia del sistema.

Per le suddette finalità, gli interventi tecnici potranno anche comportare l'accesso ai dati trattati da ciascun Utente, ivi compreso l'accesso agli archivi di posta elettronica e la verifica dei siti internet a cui hanno avuto accesso gli Utenti abilitati alla navigazione esterna.

Il suddetto personale potrà collegarsi e visualizzare in remoto il desktop delle singole postazioni, dandone preventiva comunicazione all'interessato, qualora non si pregiudichi la necessaria tempestività e l'efficacia dell'intervento tecnico.

14. Controlli

ASP Agrigento, in qualità di sola ed esclusiva proprietaria degli strumenti informatici, nonché delle informazioni e dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare in ogni momento e comunque nel rispetto dei principi di pertinenza e non eccedenza, i controlli che ritenga opportuni e necessari per le seguenti legittime finalità:

- garantire la sicurezza e preservare l'integrità delle risorse informatiche;
- evitare la commissione di illeciti;
- garantire il corretto funzionamento delle risorse informatiche;
- cooperare con forze di polizia e autorità giudiziaria.

L'Azienda garantisce che attraverso i suddetti controlli non sia effettuato alcun controllo a distanza del lavoratore.

Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con i preventivi accorgimenti tecnici adottati dal personale competente dell'ASP Agrigento (es. filtri, configurazioni di sistemi, ecc.) l'Azienda si riserva la facoltà di adottare misure che consentano la verifica di comportamenti anomali attuati attraverso le risorse informatiche. In tal caso sarà, per quanto possibile, preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

I controlli aggregati avvengono periodicamente o per ragioni di evidenza di una anomalia, sono di natura statistica e non sono ricollegabili a comportamenti leciti o illeciti del singolo utente.

Il controllo aggregato, per sua natura anonimo, può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite.

Gli unici soggetti preposti al controllo operativo degli ambienti di posta elettronica e di Internet sono gli Amministratori di Sistema.

Ai soggetti preposti corre l'obbligo di svolgere solo le operazioni strettamente necessarie al perseguimento delle finalità riconducibili alla ricerca e all'esame di situazioni anomale e alle attività di manutenzione dei sistemi.

È proibito a soggetti privi dello specifico incarico da parte dell'Azienda di effettuare qualunque genere di attività finalizzate al controllo sulla posta elettronica e sull'accesso a Internet, anche per perseguire finalità lecite.

15. Informativa agli utenti resa ai sensi dell'art. 13 del regolamento UE n. 679/2016

Ai sensi dell' art. 13 del Regolamento UE 2016/679 ed in adempimento delle Linee Guida del Garante Privacy del 1 marzo 2007, l' Azienda Sanitaria Provinciale di Agrigento, **Titolare del trattamento** dei Dati Personali (d' ora in poi, per brevità, il **"Titolare"),** informa gli Utenti, quale assegnatari di strumentazione informatica ed eventualmente abilitati ad internet e posta elettronica, connessione VPN(dipendenti, collaboratori, ecc.), che i dati personali raccolti per le finalità indicate nel presente Regolamento aziendale formeranno oggetto di trattamento nel rispetto della normativa vigente in materia di protezione dei dati personali.

In particolare, il trattamento dei dati sarà improntato al rispetto dei principi di liceità, correttezza, trasparenza, limitazione delle finalità e della conservazione, minimizzazione dei dati (i dati raccolti saranno adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità per le quali sono trattati), esattezza, integrità e riservatezza.

I dati personali degli Utenti (ad es. nome utente, indirizzo IP, registrazione degli accessi *infile log* che comprendono gli orari in cui le operazioni vengono effettuate dall'Utente ed altre informazioni relative agli accessi alle risorse informatiche), saranno trattati esclusivamente per le seguenti **finalità:**

- esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale (ad es. sicurezza del sistema informativo, assistenza tecnica e sistemistica, controllo e programmazione dei costi aziendali, ecc.);
- effettuazione di controlli per verificare il rispetto delle regole dettate con la presente Procedura interna;
- finalità difensive.

Quanto alla **base giuridica,** il trattamento dei dati personali è necessario per:

- l' esecuzione del contratto di cui l' interessato è parte;
- I'esecuzione di un compito di interesse pubblico;
- l' adempimento degli obblighi e l'esercizio dei diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro, in conformità alle norme vigenti in materia.

II conferimento dei dati personali è obbligatorio per le suddette finalità; in mancanza all'Utente non potrà essere consentito l'uso della strumentazione informatica di lavoro.
I dati saranno trattati sia in forma cartacea, che in formato digitale e con l' adozione di misure tecniche ed organizzative per assicurare adeguati livelli di sicurezza.

I dati saranno trattati da personale dipendente o da altri soggetti che collaborano con l'Azienda, tutti debitamente a ciò autorizzati dal Titolare o da un suo delegato, nonchè da soggetti appositamente designati dal Titolare quali Responsabili del trattamento dei dati personali.

I dati personali non verranno in alcun modo diffusi e potranno essere comunicati all'Autorita Giudiziaria e/o all'Autorità di Pubblica Sicurezza ed ad altri Soggetti, nei casi previsti dalla legge.

I dati personali forniti e/o acquisiti dall' Azienda Sanitaria Provinciale di Agrigento verranno conservati nel rispetto dei termini previsti dalle disposizioni di legge e dalle vigenti procedure di scarto.

Nella qualità di interessati al trattamento, gli Utenti hanno diritto di:

- ottenere I'accesso ai propri dati personali ed alle informazioni relative agli stessi;
- ottenere l'aggiornamento, la rettifica dei dati inesatti o l'integrazione di quelli incompleti;
- ottenere la cancellazione, nei casi previsti;
- ottenere la limitazione del trattamento dei dati personali che li riguardano, nei casi previsti;

- opporsi al loro trattamento, in tutto o in parte, per motivi legittimi;
- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che li riguardano forniti al Titolare del trattamento ed hanno diritto di trasmettere tali dati ad un altro Titolare del trattamento (se tecnicamente fattibile);
- proporre reclamo all'Autorita Garante per la Protezione dei dati personali, qualora nè ricorrano i presupposti, seguendo le procedure e le indicazioni pubblicate sul sito web dell'Autorita Garante www.garanteprivacy.it.

Per l'esercizio dei suddetti diritti, i soggetti interessati potranno presentare istanza in forma scritta a:

Titolare del trattamento:
Azienda Sanitaria Provinciale di Agrigento, in persona del Direttore Generale *pro-tempore*
Sede legale: Viale della Vittoria, 321Agrigento
Email: direzione.generale@pec.aspag.it

Data Protection Officer (D.P.0.)
E-mail dpo@aspag.it

16. Gestione della sicurezza dei sistemi informativi

Le copie di backup delle informazioni, del software e delle immagini dei sistemi residenti sui server aziendali devono essere effettuati dall'Amministratore di sistema e/o dal personale incaricato all'uopo, con frequenza giornaliera.

A cura dell'Amministratore di sistema è predisposto un piano di verifica periodica del corretto funzionamento delle copie di Backup .

Le informazioni e le infrastrutture IT di proprietà dell'Azienda devono essere protette dal malware. In particolare, i programmi antivirus/antimalware devono essere installati su tutti gli apparati, sia server che postazioni di lavoro e devono essere aggiomati almeno semestralmente.

Per prevenire le vulnerabilità derivanti, l'Utente deve osservare comportamenti idonei a ridurre il rischio di attacco al sistema informatico aziendale.

In particolare, ogni Utente è obbligato a controllare la presenza e il regolare funzionamento del programma antivirus/antimalware aziendale e consentire i periodici aggiomamenti dello stesso.

Qualora il programma antivirus/antimalware rilevi la presenza di un malware, l'Utente dovrà sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'Amministratore di Sistema.

L'Utente è tenuto, altresi, a verificare mediante ii programma antivirus/antimalware ogni dispositivo magnetico di provenienza estema all'Azienda prima del suo utilizzo.

La sospensione automatica della sessione di lavoro dopo un tempo minimo di inattività deve essere attivata su ogni postazione di lavoro (il sistema deve avviare un "screensaver" automatico protetto da password che oscuri la videata).

II tempo minimo di inattività è stabilito da ciascuna Struttura Organizzativa in base alle proprie esigenze di servizio.

17. Amministratore di sistema

L' Amministratore di sistema è responsabile della sicurezza del sistema informatico dell'Azienda, in rapporto al proprio ambito di operatività e competenza.
Allo stesso spetta il compito di individuare, proporre e mettere in atto misure tecniche per garantire un livello di sicurezza adeguato al rischio (art. 32 del Regolamento).

A cura dell' Amministratore di sistema sono adottate idonee misure per garantire il ripristino dell'accesso ai dati, in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a 7 giomi.

I dati particolari salvati su sistemi di archiviazione digitale devono essere cifrati attraverso idonei sistemi di protezione.

Parimenti, quando vengono trasmessi da un sistema digitale ad un altro, i dati prima della trasmissione devono essere cifrati con adeguati sistemi di cifratura.

18. Sanificazione digitale

Per il **reimpiego** e **smaltimento di rifiuti di apparecchiature elettroniche** occorre osservare un'adeguata politica di cancellazione per prevenire accessi non consentiti ai dati personali in esse contenuti.

Pertanto, per ottemperare agli obblighi imposti dal Regolamento UE 2016/679 e dal Garante per la protezione dei dati con provvedimento del 13 ottobre 2008, in caso di dismissione o cessione di apparecchiature IT, occorre cancellare in modo sicuro, definitivo e perrnanente tutte le inforrnazioni in essi presenti, utilizzando misure tecniche che consentano di garantire la loro non intelligibilità o l'effettiva cancellazione dei dati, come meglio descritte negli allegati A e B del suddetto provvedimento del Garante per la protezione dei dati.

Per quanta riguarda i supporti rimovibili contenenti dati particolari o dati giudiziari, gli stessi, se non utilizzati, devono essere distrutti o resi inutilizzabili; pertanto possono essere riutilizzati da altri soggetti solo se le inforrnazioni precedentemente in essi contenute non sono piu intelligibili, ne in alcun modo tecnicamente ricostruibili.
E' compito dell' Amministratore di sistema e del personale eventualmente incaricato del servizio (anche estemo) di curare la suddetta attività di sanificazione digitale, su richiesta dei Direttori di Struttura.

19. Comunicazione di dati personali

L'Utente può effettuare la comunicazione di dati personali a terzi, pubblici e privati, solo qualora sia espressamente consentito da una specifica disposizione di legge o di regolamento.
Anche in tal caso, deve fare particolare attenzione ad evitare ii trattamento dei dati personali qualora le finalità da perseguire possano essere realizzate mediante l'utilizzo di dati anonimi o

con opportune tecniche di crittografia.

20. Gestione del *Data Breach*

II Data Breach è *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"* dal Titolare del trattamento.

Poichè a norma dell'art. 33 del Regolamento Europeo 2016/679 ogni violazione di sicurezza che comporti un rischio per i diritti e le liberta delle persone fisiche deve essere notificata all'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro **72 ore,** dal momento in cui il Titolare e

venuto a conoscenza della violazione, ogni Utente è obbligato a segnalare immediatamente ogni incidente (ad es. malfunzionamento PC, furto, ecc.) seguendo le istruzioni contenute nella **Procedura aziendale di gestione delle violazione di dati *(Data Breach),*** pubblicata sul sito internet aziendale nella pagina dedicata alla Privacy, al quale si fa rinvio.

21. Sanzioni

La violazione delle disposizioni della presente procedura espone ogni *Utente* a responsabilità di carattere penale e civile, con conseguente risarcimento di eventuali danni causati all'Azienda a terzi.

Nel caso in cui l'Utente sia dipendente della Azienda, saranno irrogate nei suoi confronti le sanzioni disciplinari previste dal CCNL di categoria e dal Codice Disciplinare Aziendale, all'esito del procedimento disciplinare attivato.

L'Utente si impegna a tenere indenne l' Azienda da qualsiasi danno, perdita, responsabilità, nonchè dagli oneri di spesa che dovessero derivare da atti, fatti, comportamenti non corretti o illeciti o omissioni allo stesso imputabili, in quanto è personalmente responsabile dell'utilizzo delle risorse informative affidatigli, dei dati trattati per finalità aziendali, nonchè dell'adozione di tutte le misure di sicurezza necessarie a prevenire eventuali violazioni di dati.

22. Norme finali

La procedura in questione, nel dettare una disciplina per l'utilizzo degli strumenti informatici aziendali, vuole costituire un utile strumento per sensibilizzare il personale di questa Amministrazione ad un corretto utilizzo delle risorse informatiche messe a disposizione, nel rispetto dei diritti e dei doveri di ciascuna parte, sanciti nelle norme sopra richiamate.

23. Diffusione della procedura

La presente procedura dovrà essere divulgata in modo capillare, mediante la pubblicazione sul sito aziendale e verrà sottoposta ad aggiornamento periodico.

24. Rinvio

Per quanto non previsto, si fa riferimento alle vigenti disposizioni legislative e regolamentari in materia di protezione dei dati personali ed alle disposizioni civili e penali vigenti in materia.