SERVIZIO SANITARIO NAZIONALE REGIONE AUTONOMA FRIULI-VENEZIA GIULIA

AZIENDA PER L'ASSISTENZA SANITARIA N. 3
"ALTO FRIULI-COLLINARE-MEDIO FRIULI"

TESTO UNICO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Ai sensi D.Lgs. 196/03 " Codice in materia di protezione dei dati personali"e succ. mod. e integr.

Anno 2015

SOMMARIO

Parte I - Guida al codice privacy (D.Lgs. 196/2003)
Consigli utili per lavorare nel rispetto della privacy

Parte II - Policy per l'utilizzo delle risorse informatiche

Parte III – Servizio di accesso a Internet tramite Wi-Fi

Parte I - Guida al codice privacy (D.Lgs. 196/2003)
Consigli utili per lavorare nel rispetto della privacy

Introduzione

Con il D.lgs. 30 giugno 2003 n. 196 è stato approvato Il "Codice Privacy" - Testo Unico in materia di Protezione dei Dati Personali.
Questo provvedimento riunisce ed integra tutte le varie disposizioni già emanate in materia, prima fra tutte la Legge 675/96 che, per prima in Italia, ha regolamentato l'uso dei dati personali garantendo che il trattamento dei dati medesimi si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.
Le fonti normative che hanno contribuito a dare origine al substrato normativo del Codice privacy si rinvengono nell'art. 2 della Costituzione " La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità….", il successivo art. 13 della Fonte costituzionale " la libertà personale è inviolabile….", l'art. 32"….nessuno può essere obbligato a un determinato trattamento sanitario se non per disposizione di legge….".

Definizioni

Per trattamento s'intende qualunque operazione concernente in generale la raccolta, l'elaborazione, il raffronto, la modificazione, l'estrazione, la comunicazione e/o diffusione, la conservazione e la distruzione dei dati.

In particolare s'intende per:

- raccolta - il momento in cui avviene l'acquisizione dei dati da parte dell'amministrazione;
- elaborazione - il processo immediatamente successivo alla raccolta dei dati, inerente le operazioni di organizzazione dei dati medesimi;
- raffronto - l'operazione di comparazione tra dati;
- modificazione - la variazione dei dati in seguito a nuova acquisizione, l'aggiornamento;
- estrazione – l'estrapolazione o la duplicazione di dati precedentemente selezionati;
- comunicazione – il dare conoscenza di dati personali ad uno o più *soggetti determinati diversi dall'interessato*, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- diffusione - il dare conoscenza di dati personali a *soggetti indeterminati (ossia a chiunque)*, in qualunque forma , anche mediante la loro messa a disposizione o consultazione.

I soggetti interessati all'applicazione del Codice

I principali soggetti interessati all'applicazione del Codice sono:

a) il Titolare del trattamento dei dati personali
b) il Responsabile del trattamento
c) l'Incaricato del trattamento
d) l'Interessato
e) il Garante

a-T*itolare del trattamento dei dati personali*

Il Titolare del trattamento è, ai sensi dell'articolo 29 del Codice, la persona fisica o giuridica, la Pubblica Amministrazione nel suo complesso e qualsiasi altro Ente, associazione od organismo cui spettano le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, anche sotto l'aspetto della sicurezza.

Esso provvede a:
- nominare i Responsabili del trattamento di dati, impartendo loro le necessarie istruzioni per la corretta gestione e tutela dei dati personali;
- assolvere l'obbligo della notificazione al Garante;
- adottare le misure di sicurezza necessarie per garantire la sicurezza dei dati personali;
- verificare periodicamente l'osservanza dell'attività svolta dai Responsabili del trattamento rispetto alle istruzioni impartite
- adotta annualmente il Documento programmatico sulla sicurezza (DPS).

Il Titolare ha facoltà di delegare alcuni dei propri compiti al Responsabile (nominare gli incaricati, coordinare l'uso dei dati, controllare il rispetto delle disposizioni).

Nell' AAS n° 3 "Alto Friuli" la funzione di Titolare è svolta dal Direttore Generale pro-tempore, rappresentante legale dell'Ente.

b-R*esponsabile del trattamento*

Il Responsabile del trattamento opera in esecuzione delle disposizioni della specifica normativa, di altre disposizioni impartite dal Direttore Generale, secondo le regole consigliate dall'esperienza e dal buon senso.
Il Responsabile compie tutto quanto è necessario per assicurare il rispetto delle vigenti disposizioni in tema di riservatezza, adottando le precauzioni individuate nel piano di sicurezza dei dati personali elaborato dall'Azienda.
Le funzioni di responsabile non sono delegabili e i responsabili sono tenuti a nominare per iscritto gli incaricati indicando l'ambito dei trattamenti consentiti e le attività eseguibili, aggiornando annualmente le loro nomine.

Il Responsabile ha i seguenti principali compiti:
a) nomina gli incaricati al trattamento;
b) verifica che oggetto del trattamento siano solo i dati essenziali (pertinenti, non eccedenti) per lo svolgimento della propria attività istituzionale, che i dati personali vengano trattati in modo corretto e vengano raccolti e registrati per scopi determinati;
c) verifica che gli operatori addetti forniscano all'interessato per iscritto l'informativa e acquisiscono il consenso (ove richiesto) secondo le procedure ed attraverso i modelli forniti dalla Direzione aziendale;
d) verifica la conservazione e sicurezza degli archivi amministrativi cartacei e non, con riferimento ai dati oggetto dei trattamenti di competenza.

Nell'AAS n° 3 i Responsabili del trattamento sono stati identificati, con delibera n° 23 del 29/01/2015 nei Responsabili di SOC e SOS Dipartimentali aziendali.

c-I*ncaricato del trattamento*

Gli Incaricati al trattamento sono nominati per iscritto dal Responsabile del trattamento i conformità e secondo i criteri identificati con delibera n° 23 del 29/01/2015.
Sono tenuti ad eseguire i trattamenti secondo le disposizioni riportate nell'atto di nomina e comunque nell'ambito del trattamento consentito, intendendo per esso "*le sole ed esclusive finalità afferenti l'attività istituzionale dell'unità organizzativa di appartenenza, collegando il profilo di autorizzazione alla qualifica e ruolo rivestiti all'interno della struttura organizzativa medesima*".

I principali compiti dell'incaricato sono:

1. verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Responsabile;
2. trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
3. conservare i dati rispettando le misure di sicurezza previste dalla normativa vigente nonché quelle predisposte dall'Azienda e/o dal Responsabile, garantendo la massima riservatezza in ogni operazione di trattamento;
4. comunicare a terzi i dati solo a fronte di preventiva e specifica autorizzazione del Responsabile del trattamento;
5. rispettare la massima riservatezza sui dati personali dei quali vengano a conoscenza nello svolgimento dell'incarico per tutta la durata del medesimo e anche successivamente il termine stesso;
6. informare immediatamente il Responsabile del trattamento della cessazione per qualsiasi causa (distruzione accidentale, termine della sperimentazione, necessità di trasferimento di archivi, chiusura del trattamento) del trattamento dei dati.

d-I*nteressato*

L'Interessato è la persona cui si riferiscono i dati personali oggetto del trattamento. E' titolare delle informazioni che lo riguardano e dunque ha diritto :

1. di conoscere l'esistenza di trattamenti di dati che lo riguardano;
2. di ottenere la cancellazione, la trasformazione in forma anonima od il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
3. di ottenere l'aggiornamento, la rettificazione ovvero, qualora vi abbia interesse, l'integrazione dei dati;
4. di conoscere le finalità per le quali il trattamento viene effettuato;
5. di essere messo a conoscenza delle conseguenze della mancata prestazione del consenso.

In sintesi l'interessato ha diritto:

- all'informazione (art. 13);
- all'accesso dei suoi dati (art. 7);
- all'opposizione (per motivi legittimi, per il compimento di ricerche di mercato o di comunicazione commerciale).

e- *Garante*

E' un organo collegiale composto da 4 membri, eletti dal Parlamento, al cui interno viene eletto un Presidente. L'Organo è preposto al controllo del corretto utilizzo dei dati personali ed alla applicazione delle sanzioni previste per legge.
Il Garante ha poteri amministrativi di vigilanza e controllo, sanzionatori e decisori; ha compiti collaborativi e dovere di relazionare al Governo e al Parlamento.

Il Garante può disporre accessi ed ispezioni alle banche dati o richiedere l'effettuazione di rilevazioni nei luoghi dove si svolgono i trattamenti nonché chiedere informazioni ed esibizione di documenti (anche con il supporto dei NAS, della Guardia di Finanza).

Ogni interessato che ritenga lesi i propri diritti nell'esecuzione del trattamento dei suoi dati personali può fare ricorso all'Ufficio del Garante.

Dati personali

Per "dato personale" si intende qualunque informazione relativa a persona fisica, giuridica, identificati o identificabili, anche indirettamente, ivi compreso un numero di identificazione personale (es. nome, cognome, indirizzo, partita iva, codice fiscale, ecc.)

NO CONSENSO

Per questi dati non serve acquisire il consenso dell'interessato quando il trattamento è legato allo svolgimento delle funzioni istituzionali dell'Azienda sanitaria.

SI' INFORMATIVA

L'informativa (art. 13) deve invece essere rilasciata al momento della raccolta dei dati personali e costituisce una condizione necessaria per l'esercizio dei diritti di cui all'art. 7.

Comunicazione dei dati personali a soggetti pubblici

La comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico è ammessa solo se prevista da legge, da regolamento o necessaria per lo svolgimento di funzioni istituzionali.

Dati sensibili e giudiziari

Per "dati sensibili" si intende i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, *nonché i dati personali idonei a rivelare lo stato di salute (dati sanitari)* e la vita sessuale.

Per "dati giudiziari" si intende i dati personali idonei a rivelare i provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o indagato ai sensi degli artt. 60 e 61 c.p.p.

Trattamento dei dati sanitari (art. 76 D.Lgs. 196/03)

SI' INFORMATIVA

L'informativa (art. 13) deve essere sempre rilasciata all'interessato al momento della raccolta dei dati personali e costituisce una condizione necessaria per l'esercizio dei diritti di cui al citato art. 7.

SI' CONSENSO

Per il trattamento dei dati sanitari è SEMPRE necessario acquisire il consenso dell'interessato, tranne:

- quando le finalità di cura e salute riguardino un terzo o la collettività;
- nei casi di urgenza ed indifferibilità della cura a tutela della salute dell'interessato.

In tali due ultimi casi il consenso dovrà essere richiesto al primo momento utile.

Artt. 39 - 110

Quando il trattamento dei dati idonei a rivelare lo stato di salute è finalizzato a scopi di ricerca scientifica (in campo medico, biomedico, epidemiologico) prevista dalla legge o che rientra in un programma di ricerca biomedica e sanitaria previsto ai sensi dell'art. 12-bis del D.Lgs. 502/1992 e ss. mm. :

a) non è necessario il consenso dell'interessato;
b) occorre però che il Titolare del trattamento ne dia comunicazione (preventiva) al Garante e inizi il trattamento stesso solo dopo 45 gg. dalla comunicazione (salvo ovviamente ricevimento del diniego da parte del Garante).

I dati idonei rivelare lo stato di salute non possono mai essere diffusi (ossia comunicati a soggetti indeterminati – a "chiunque").

I dati idonei rivelare lo stato di salute possono essere resi noti all'interessato solo tramite il medico designato dal Titolare o dall'interessato (o altro esercente la professione sanitaria autorizzato, che ha rapporti diretti con i pazienti).

Il diritto di accesso ai dati (art. 7)

Sintesi dell'art. 7 ("Diritto di accesso ai dati personali ed altri diritti"):

Il soggetto interessato, ovvero colui al quale il dato stesso si riferisce ed appartiene, ha diritto di ottenere:

- la conferma dell'esistenza o meno di dati personali che lo riguardano;
  l'indicazione dell'origine dei dati personali; delle finalità e modalità del trattamento; delle modalità del trattamento (cartaceo – informatico); degli estremi identificativi del titolare (e di eventuali altri soggetti – c.d. responsabili e/o incaricati – delegati dall'ente stesso al trattamento); dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza;
- l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
- L'interessato ha diritto di opporsi, in tutto o in parte: a) per motivi legittimi; b) per fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

La richiesta potrà essere effettuata dall'interessato senza particolari formalità (oralmente, per iscritto, via fax ecc.) anche attraverso un soggetto delegato dallo stesso.

Si deve rispondere alla richiesta entro 15 gg. (massimo 30 gg. con giustificato motivo), altrimenti l'interessato "non soddisfatto" può presentare ricorso al Garante.

Informativa (art. 13)

L'interessato deve essere previamente informato circa:

1. le finalità e le modalità del trattamento cui sono destinati i dati;
2. la natura obbligatoria o facoltativa del conferimento dei dati; le conseguenze di un eventuale rifiuto di rispondere;
3. i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati,
4. l'ambito di diffusione dei dati medesimi;
5. i diritti di cui all'articolo 7;
6. gli estremi identificativi del Titolare (e del Responsabile).

Attraverso l'informativa, l'interessato può esercitare un controllo diretto sull'operato del soggetto (incaricato) che effettua il trattamento dei suoi dati.

L'obbligo di informativa viene assolto oltre che con cartellonistica esposta nei punti di maggior affluenza/attesa dell'utenza, con modulistica informativa e dettagliata, messa a disposizione presso i punti CUP dei presidi ospedalieri, dei punti informazione, le sale di attesa e le segreterie degli ambulatori.

La notifica

La notificazione è la dichiarazione con la quale il Titolare del trattamento rende nota al Garante l'esistenza di un'attività di raccolta e utilizzazione dei dati personali specificati nell'art. 7 del codice privacy.

Le misure di sicurezza

Le misure di sicurezza sono un complesso di misure tecniche, logistiche, organizzative, informatiche, procedurali che hanno la funzione di proteggere i dati dal pericolo di distruzione anche accidentale, perdita, manipolazione, utilizzo improprio, illecito.
Le misure di sicurezza si distinguono in:

- minime: quelle che rappresentano il livello minimo di protezione imposto dalla legge (per evitare le sanzioni penali previste);
- idonee: non sono codificate, sono scelte e sviluppate dal Titolare in base alla valutazione del rischio. Il concetto di idoneità è ancorato anche all'evoluzione tecnologica: pertanto tali misure devono essere periodicamente verificate e aggiornate (se tali misure vengono valutate – ex post – non idonee, l'Azienda è comunque civilmente responsabile dei danni causati all'interessato per il trattamento dei suoi dati personali in modo "non idoneo").

Con l'art. 45 del D.L. n° 5 del 09/02/2012" Decreto semplificazioni" è stato eliminato l'obbligo per il Titolare del trattamento dei dati di redigere e aggiornare entro il 31/03 di ogni anno il Documento Programmatico per la Sicurezza contemplato dall'art. 34, 1 bis del D.Lgs. 196/03, mantenendo altresì invariato l'obbligo di definire in un documento e rispettare tutte le altre misure di sicurezza contemplate dal Codice Privacy, tal essendo:

- redazione idonee informative (art. 13 D.Lgs. 196/03);
- nomina responsabili al trattamento dei dati personali, compresi trattamenti affidati in outsourcing (art. 29 D.Lgs. 196/03);
- nomina incaricati al trattamento dei dati personali (art. 30 D.Lgs. 196/03);
- regolamento interno per uso internet e posta elettronica (art. 154, comma 1, lett. c) D.Lgs 196/03);
- nomine e prescrizioni in tema di Amministratori di Sistema (art. 154, comma 1, lett. c) e h) D.Lgs. 196/03);
- prescrizioni in materia di videosorveglianza (art. 154, comma 1 , lett. c) –D.Lgs. 196/03 – provvedimento garante privacy 08/04/2010);
- policy sito web e servizi interattivi;
- formazione del personale.

La tutela avanti al Garante e la tutela giurisdizionale:
strumenti di difesa per il soggetto "interessato".

Gli strumenti di tutela a disposizione del soggetto cui si riferiscono i dati oggetto del trattamento (si ricordi che "interessato" non è solo la persona fisica ma può essere anche una persona giuridica e quindi l'ente associativo, i cui dati sono sottoposti a trattamento da terzi) sono diversi. Sinteticamente e sommariamente si elencano di seguito.

Davanti al Garante l'interessato potrà proporre:
- un reclamo al fine di rappresentare una qualsiasi violazione in materia di trattamento di dati personali;
- una segnalazione di eventuali violazioni della disciplina in materia di privacy;
- il ricorso amministrativo per denunciare la violazione delle norme contenute nel nuovo codice della privacy e in particolar modo per ottenere tutela in ordine ai diritti di cui all'art. 7 D.lgs. 196/2003.

Il ricorso al Garante e il ricorso all'autorità giudiziaria sono tra loro alternativi, la scelta quindi è lasciata al soggetto interessato.

Disposizioni per il controllo e la custodia degli atti e dei documenti:

- per tutto il periodo in cui i documenti sono all'esterno dei luoghi di custodia, l'incaricato è responsabile della custodia dei documenti stessi. È importante ricordarsi di chiudere a chiave armadi, cassetti ecc. nei quali vengono conservati i dati personali;
- si deve porre particolare attenzione nell'utilizzo delle stampanti di rete, in particolare quando queste sono poste in luoghi il cui accesso non è controllato, recuperando immediatamente i documenti stampati quando questi contengono dati personali;
- non abbandonare documenti fotocopiati o l'originale presso le fotocopiatrici. Eventuali fotocopie non riuscite bene o non più necessarie debbono essere distrutte in un apposito trita documenti, se disponibile, oppure devono essere strappate in pezzi talmente piccoli da non consentire in alcun modo la ricostruzione del contenuto. È sconsigliabile utilizzare le fotocopie non riuscite come carta per appunti;
- quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l'incaricato deve porre particolare attenzione alla custodia della cartella o della borsa nella quale i documenti sono contenuti;
- è tassativamente proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il corrispondente sia un incaricato il cui profilo di autorizzazione sia tale da potere trattare i dati in questione.
- si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono in presenza di terzi non autorizzati. Queste precauzioni diventano particolarmente importanti quando il telefono è utilizzato in luogo pubblico od aperto al pubblico;
- in particolare nei presidi ospedalieri attenersi strettamente alle indicazioni fornite dagli utenti nella parte a ciò dedicata del modulo per l'acquisizione del consenso, quanto al rilascio di informazioni a terzi sullo stato di salute dell'assistito, nonché sulla presenza e allocazione all'interno dei presidi ospedalieri.

Misure per il rispetto dei diritti degli interessati:

- Il titolare adotta idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati sensibili e di misure minime di sicurezza.
- Dette misure comprendono in particolare:
  - soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno delle strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
  - l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
  - soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
  - cautele volte ad evitare che le prestazioni sanitarie avvengano in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
  - il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;

- la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;
- la formale previsione di adeguate formalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informando previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;
- la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei, un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
- la sottoposizione degli incaricati non tenuti per legge al segreto professionale a regole di condotta analoghe allo stesso.

I vantaggi della privacy

L'introduzione di una legge sul trattamento dei dati personali è un segnale di civiltà e di rispetto sia verso gli utenti già assistiti sia verso i potenziali.

Ci sono tuttavia anche altre considerazioni pratiche che ne rendono efficace l'applicazione:

- *valorizzazione dei propri archivi:*

la normativa sulla privacy comporta da parte delle Aziende sanitarie principalmente un attento censimento dei propri dati e la verifica delle misure di sicurezza esistenti. Questo adempimento è spesso un'ottima occasione per migliorare flussi interni e qualità dei dati;

- *miglioramento immagine e qualità aziendali:*

l'Azienda sanitaria che applica la legge sulla privacy informando correttamente l'interessato godrà sicuramente di una migliore immagine e di un maggior rapporto di fiducia verso l'utenza, rispetto all'Azienda che non la applica.

In conclusione il rispetto del Codice della Privacy consente all'Azienda sanitaria di migliorare:
- qualità del rapporto tra cittadini /PA;
- funzionalità dei servizi offerti;
- rendere trasparente la gestione dei dati del cittadino.

Parte II - Policy per l'utilizzo delle risorse informatiche

Premessa

La crescente diffusione delle tecnologie dell'ICT (Information and Communication Technology) ha portato da un lato ad un significativo aumento della produttività e della qualità del lavoro svolto, dall'altro ha determinato l'aumento dei rischi di violazione della privacy e della sicurezza.
Di seguito si riporta un insieme di norme e di linee guida da seguire per eliminare o ridurre i rischi derivanti da un uso poco corretto o poco consapevole delle risorse informatiche e telematiche messe a disposizione dall'Azienda per l'Assistenza Sanitaria n° 3 "Alto Friuli – Collinare – Medio Friuli".
Il ulteriore obiettivo del documento è quello di chiarire alcuni aspetti fondamentali relativi alle modalità e alle condizioni di utilizzo delle risorse informatiche di AAS 3, al fine di migliorarne l'efficienza d'uso, di garantire tempestività nell'attività di assistenza tecnica e di recepire indicazioni essenziali per gli sviluppi futuri del sistema informativo.
La policy si ispira ai seguenti principi:

- l'utilizzo delle risorse informatiche e telematiche, come quello di qualsiasi strumento aziendale, deve sempre ispirarsi ai principi di diligenza e correttezza impliciti nell'ambito del rapporto di lavoro;

- una percentuale significativa delle violazioni delle leggi sulla sicurezza e sulla privacy avviene in modo inconsapevole o comunque non doloso, come conseguenza di una scarsa informazione e della carenza di norme scritte e dettagliate;

- in molto casi le prime "vittime" della violazione della privacy e della sicurezza sono i dipendenti stessi; da questo punto di vista il presente documento vuole innanzi tutto tutelare e salvaguardare il dipendente, che con certi strumenti (Internet, posta elettronica, etc.) deve convivere per una percentuale significativa del suo tempo

- particolare enfasi è stata data all'utilizzo di Internet e della posta elettronica, non solo per l'importanza che questi strumenti rivestono come mezzi di comunicazione, ma anche e soprattutto per le implicazioni di carattere tecnico-legale ed organizzativo che il loro uso comporta.

Questo documento contiene le linee guida e le regole di comportamento da adottare nell'utilizzo dei sistemi informatici aziendali per proteggere le risorse informatiche stesse e i dati in esse contenuti con riferimento in particolare alle misure di sicurezza imposte per il trattamento di dati personali dal D.P.R. 196/03.

Finalità della Policy

Le finalità di questo documento sono:

a) garantire e salvaguardare la sicurezza e la privacy dei dipendenti dell' AAS 3;

b) stabilire una policy per la sicurezza e il rispetto della privacy nell'utilizzo dei sistemi informatici aziendali, con riferimento in particolare alle misure di sicurezza imposte dalle normative per il trattamento di dati personali;

c) fornire idonee indicazioni ed istruzioni a tutto il personale interessato dalle predette misure di sicurezza;

d) regolamentare l'utilizzo delle risorse informatiche in modo che siano utilizzate in modo efficace, produttivo, e orientato al raggiungimento degli obiettivi aziendali; garantire la sicurezza e prevenire il danneggiamento delle risorse informatiche, dei servizi e delle attività legate all'utilizzo di Internet e della posta elettronica;
e) garantire e salvaguardare la sicurezza e la privacy dei dipendenti dell' AAS 3.

Ambiti di applicazione

Questa policy si applica:

a) a tutti gli utenti che utilizzano le risorse informatiche dell'AAS 3, siano essi dipendenti a tempo pieno o parziale, collaboratori, consulenti, dipendenti di aziende esterne legate da contratti di fornitura di servizi o altri individui a cui ne è concesso l'uso;

b) a tutte le risorse informatiche di proprietà dell'AAS 3;

c) a tutte le operazioni di accesso a informazione registrate ed archiviate elettronicamente tramite risorse informatiche aziendali;

d) a tutte le forme di comunicazione operate attraverso Internet e la posta elettronica.

Verifiche

Salvo l'obbligo per ciascun utente dell' AAS 3 di seguire la Policy e di segnalarne eventuali violazioni al Responsabile del Sistema Informativo Aziendale, le funzioni di verifica del rispetto sono assegnate all'Ufficio Sistemi Informativi.
Tutti gli utenti sono tenuti a segnalare prontamente qualsiasi violazione alla presente policy. Non sono ammesse segnalazioni di violazioni in forma anonime, a meno che non risultino correlate a particolari tipologie di reati contro la Pubblica amministrazione rientranti nella fattispecie dei reati contemplati dal Cap. II.,Titolo II C.P.
Viene comunque tutelato dall'AAS3 il diritto alla privacy degli utenti che comunicassero dette violazioni nei limiti previsti dalla normativa italiana, nonché dalle disposizioni in materia di anticorruzione di cui alla L. 190/12 , nonché dal Piano aziendale per la prevenzione della corruzione.

Sanzioni

Poiché, in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'AAS3 verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio Sistema Informativo.

In caso di violazione accertata del presente regolamento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali. Qualsiasi violazione alla normativa italiana vigente da parte degli utenti sarà segnalata alle autorità competenti.

Definizioni dei termini maggiormente utilizzati

E' utile definire i termini maggiormente ricorrenti nel documento e le definizioni tecniche che potrebbero essere difficilmente comprensibili all'utenza media.

Comunicazione elettronica: qualsiasi comunicazione creata, inviata, inoltrata, trasmessa, archiviata, copiata, scaricata, mostrata, vista o stampata da uno o più sistemi o servizi di comunicazione elettronica.
Policy o Regolamento: documento che ha ad oggetto la regolazione di una determinata funzione aziendale. Può inoltre contenere delle linee guida e dei suggerimenti per una migliore fruizione dei servizi aziendali.
Responsabile del sistema informativo aziendale: il responsabile della sicurezza e della gestione delle Risorse informatiche aziendali.
Risorse informatiche aziendali: qualsiasi combinazione di apparati tecnologici dell'Azienda Sanitaria n. 3 "Alto Friuli" e del SISSR hardware o software utilizzati per le comunicazioni elettroniche ed elaborazione dei dati.
Situazione d'emergenza: circostanza nella quale il venir meno di un'azione può provocare un serio pregiudizio a persone o cose, comportare il danneggiamento o la scomparsa di dati o impedire la verifica di una grave responsabilità dell'Azienda Sanitaria n. 3 "Alto Friuli" o di qualche dipendente dell'Azienda.

Utente: ciascuna persona che acceda alle Risorse informatiche aziendali.
SISSR: complesso dell'infrastruttura telematica, delle procedure applicative condivise con tutte le aziende sanitarie della Regione Friuli Venezia Giulia.
INSIEL: la società concessionaria che si occupa della realizzazione degli sviluppi e della conduzione del SISSR.

Utilizzo delle risorse informatiche aziendali

Utilizzatori.

L'utilizzo delle risorse informatiche aziendali e di quelle messe a disposizione dal SISSR è riservato ai dipendenti dell'AAS 3 e ad altri soggetti espressamente autorizzati dal Responsabile della Struttura di appartenenza. Il Responsabile della Struttura si occupa di richiedere al Responsabile del sistema Informativo l'abilitazione ai servizi informatici e l'accesso alle banche dati necessari a ciascun utente, comunicando prontamente qualsiasi modifica relativa all'organico che richieda l'attivazione o la sospensione di servizi informatici o autorizzazione all'accesso alle banche dati.

Utilizzi consentiti

a) Le risorse informatiche aziendali sono strumenti di lavoro e come tali possono essere utilizzate solo per scopi strettamente professionali e lavorativi. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, ecc.), sia per quelle affidate al singolo dipendente (PC, periferiche, stampanti locali, …). Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.

b) Le risorse informatiche affidate al singolo dipendente (es. personal computer fisso o mobile e i relativi programmi e/o applicazioni) sono strumenti di lavoro appartenenti al patrimonio aziendale e pertanto vanno custoditi in modo appropriato; il furto, il danneggiamento o lo smarrimento di tali strumenti debbono essere prontamente segnalati all'azienda.

c) In caso di trasferimento d'ufficio o di funzione, tutte le strumentazioni tecniche restano in uso presso la stessa Struttura salvo esplicita autorizzazione da parte del responsabile della Struttura di appartenenza.

Gestione delle password di accesso

a) L'accesso alle risorse elaborativi aziendali (personal computer, terminali, reti locali, applicativi, basi dati, etc.) è protetto da password che devono essere custodite dall'incaricato con la massima diligenza e non possono essere divulgate per nessun motivo.

b) Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Responsabile del Sistema Informativo aziendale.

Configurazioni di sistema

Non è consentito modificare le configurazioni impostate sul PC affidato. Di norma ogni PC aziendale, deve essere collegato alla rete telefonica. Casi particolari di non connessione vanno esplicitamente autorizzati dal responsabile del Sistema Informativo.

Installazione di hardware/software

a) Non è consentita l'installazione di programmi provenienti dall'esterno dell'azienda, salvo previa autorizzazione esplicita del Responsabile del Sistema Informativo aziendale. L'installazione autonoma di software non autorizzato comporta un grave pericolo di introduzione di virus informatici e/o di alterazione della stabilità delle applicazioni presenti nell'elaboratore.

b) Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dall'AAS 3 o resi disponibili in ambito SISSR (D.lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).

c) Non è consentita l'installazione autonoma di alcun dispositivo di memorizzazione, comunicazione o altro (es. masterizzatori, modem, …), se non con l'autorizzazione esplicita del Responsabile del Sistema Informativo aziendale.

d) Non sono consentiti l'istallazione e/o l'utilizzo di strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o di documenti informatici.

Supporti magnetici

a) Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, DVD, nastri magnetici di provenienza ignota o dubbia.

b) Ogni dispositivo magnetico di provenienza esterna all'AAS3 dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, l'utente dovrà avvertire tempestivamente Insiel che provvederà alla verifica e rimozione del virus.

c) Non è consentito scaricare file provenienti da Internet oppure contenuti in supporti magnetici/ottici che non abbiano una chiara attinenza con la propria prestazione lavorativa.

d) I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi a due livelli chiusi a chiave.

e) Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato anche dopo la cancellazione dei dati in essi contenuti.

f) Non è consentita la memorizzazione e la diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Connessione alla rete locale

a) 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.

b) L'AAS si riserva la facoltà di procedere alla rimozione di qualsiasi file o applicazione memorizzati sulle unità di rete in caso che li ritenga pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione della presente policy.

c) Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi compresi quelli resi disponibili attraverso server di rete, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati.

d) Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. 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.

Password per l'accesso alla rete e alle applicazioni condivise

a) Le Password di ingresso alla rete, di accesso ai programmi, sono previste ed attribuite da Insiel, previa richiesta da parte del Responsabile S.O. di afferenza all'ufficio password presso la SO Programmazione e controllo di gestione che a sua volta inoltrerà richiesta a INSIEL. Viene comunque consentita "*autonoma sostituzione da parte degli incaricati al trattamento*" (come previsto dal D.Lgs. 196/03).

b) Gli utenti sono tenuti a conservare la segretezza della propria password ed a rispettare le policy per la creazione di password sicure.

c) Gli utenti sono tenuti a sostituire immediatamente la Password, nel caso si sospetti che la stessa abbia perso la segretezza.

e) E' assolutamente proibito l'accesso alla rete locale e/o alle applicazione condivise con nomi utente diversi da quello assegnato.

f) Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più PC o terminali.

Diritti di accesso e controllo remoto

a) Per facilitare le operazioni di aggiornamento del software e per garantire la sicurezza dei dispositivi, delle applicazioni e dei dati, l'Insiel può avvalersi di strumenti di controllo remoto che consentano di compiere le operazioni necessarie attraverso la rete locale.

b) L'assistenza tecnica per malfunzionamenti ordinari o diagnosi di sistema attraverso strumenti di controllo remoto deve avvenire solo previa autorizzazione dell'utilizzatore e di norma in presenza dell'utilizzatore stesso.

c) In caso di malfunzionamenti straordinari e in situazioni di emergenza, l'Insiel o persona espressamente delegata ha la facoltà in qualunque momento di accedere a qualunque Sistema Informativo aziendale per l'espletamento delle proprie funzioni.

Insiel o persona espressamente delegata, può in qualunque momento procedere alla rimozione di qualsiasi file o applicazione che riterrà essere pericolosi per la sicurezza, sia sui PC degli incaricati sia sulle unità di rete.

Utilizzo della rete Internet e dei relativi servizi

Connessione a Internet

a) Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

b) E' fatto divieto assoluto per gli utenti connettersi autonomamente alla rete Internet con sistemi di dial-up a numeri esterni all'AAS3, salva autorizzazione del Responsabile del Sistema Informativo aziendale.

c) E' vietato per l'utente modificare le impostazioni del Web Browser stabilite dall'Insiel.

Navigazione Internet

a) È fatto divieto assoluto scaricare programmi, o contenuti multimediali senza la previa autorizzazione del Responsabile del Sistema Informativo aziendale.

b) L'Insiel, per conto dell'AAS 3 può effettuare il monitoraggio dei siti visitati dai dipendenti al fine di ridurre i tempi e i costi di navigazione ed ha facoltà di porre limiti alla navigazione internet escludendo dalla navigazione siti non attinenti agli scopi aziendali.

c) Qualora si reputi necessario trasmettere via web dati sensibili o informazioni riservate via Web è necessario accertarsi che vi sia la protezione della comunicazione attraverso il sistema crittografico SSL (Secure Socket Layer). Ciò può essere verificato controllando che nel bordo inferiore destro del browser appaia il disegno di un piccolo lucchetto giallo chiuso.

d) Gli utenti sono invitati a limitare il rilascio di informazioni personali durante la navigazione via Web. L'utente è tenuto nel corso della navigazione a leggere con attenzione qualsiasi finestra, pop up o avvertenza prima di proseguire nella navigazione e in particolare prima di accettare delle condizioni contrattuali o di aderire a delle iniziative online.

e) 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 direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

f) È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

g) È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (nickname).

Utilizzo della posta elettronica

Utilizzi consentiti

La casella di posta, assegnata dall'AAS3 all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

a) È fatto divieto di scaricare sul computer locale o sulle risorse condivise in rete messaggi di posta elettronica di caselle diverse da quelle assegnate dall'AAS 3 all'utente.

b) Non è consentito utilizzare la posta elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate In particolare è fatto divieto di utilizzare le risorse informatiche per la comunicazione elettronica ed in particolare le caselle di posta elettronica aziendale ……@ass3.sanita.fvg.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

c) La casella di posta elettronica aziendale anticorruzione@ass3.sanita.fvg.it creata secondo i dettami del Piano aziendale di prevenzione della corruzione ex L. 190/12, deve essere utilizzata ai soli fini di tutela del wistleblowing come previsto dalla norma medesima.

d) È fatto divieto di utilizzare le risorse informatiche per la comunicazione elettronica in modo anonimo o modificando la reale identità del mittente.

e) Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

f) La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare documenti di lavoro "strettamente riservati";

g) Poiché in caso di violazioni contrattuali e giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Insiel, per conto dell'AAS3 verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio Sistema Informativo.

h) L’utente è tenuto a seguire attentamente le disposizioni date dall’Ufficio Sistemi Informativi riguardo alla protezione da virus e da altri software pericolosi per il Sistema Informativo aziendale. Deve essere cura di ogni utente verificare che il software antivirus sia attivo.

i) Nel caso che 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 al responsabile aziendale per il servizio informatico.

Contenuto dei messaggi

a) Gli utenti devono prestare attenzione nell’invio di messaggi elettronici affinché non siano inserite inconsapevolmente delle informazioni su User e Password utilizzate in altre applicazioni. In particolare va usata la massima cautela nell’invio a mezzo posta elettronica di pagine internet che potrebbero contenere nell’indirizzo informazioni utili a risalire alla User/Password utilizzata.

b) Gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi.

c) E’ esplicitamente vietato l’invio di messaggi in risposta a richieste di adesione a programmi di catene di e-mail, indipendentemente dalle finalità presunte.

d) Gli utenti sono invitati a limitare l’uso della funzione “Rispondi a tutti” nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari.

Gestione delle liste di destinatari

Gli utenti devono prestare attenzione nell’organizzazione dell’agenda del proprio client di posta affinché non vi possano essere degli errori nella selezione dei destinatari dei messaggi.

Confidenzialità della posta elettronica

La confidenzialità della posta elettronica e della comunicazione attraverso il Web è limitata, in quanto i messaggi transitando nella rete pubblica di Internet possono essere visionati da terzi non autorizzati. Il livello di confidenzialità di una e-mail si avvicina di più a quello di una cartolina piuttosto che a quello di una lettera. Per questa ragione è fatto divieto assoluto di comunicare informazioni classificate come riservate o dati sensibili attraverso l’e-mail o attraverso il Web se non esplicitamente autorizzati dalla Direzione dell’Azienda.
Si raccomanda di prevedere, con la funzione di inserimento automatico della firma in calce all’e-mail, la seguente avvertenza sulla privacy e sulla confidenzialità dei messaggi inviati: ”*Questo messaggio è di carattere riservato ed è indirizzato esclusivamente al destinatario specificato. L'accesso, la divulgazione, la copia o la diffusione sono vietate a chiunque altro ai sensi delle normative vigenti, e possono costituire una violazione penale. In caso di errore nella ricezione, il*

ricevente è tenuto a cancellare immediatamente il messaggio, dandone conferma al mittente a mezzo e-mail. "
Si raccomanda agli utenti di prestare la massima attenzione nella stampa di messaggi di posta elettronica soprattutto nel caso si utilizzino delle stampanti di rete o accessibili a più persone.

Best Practices per l'utilizzo della posta elettronica

a) Gli utenti sono invitati a leggere quotidianamente la posta elettronica e a rispondere in tempi ragionevoli alle e-mail ricevute.
b) Gli utenti sono tenuti sempre ad accertarsi che gli eventuali allegati dei propri messaggi non eccedano la dimensione massima di 10 Mb lordi (7 mb netti). Qualora si riscontrasse la necessità di allegare un file di dimensioni superiori è buona norma ridurre le dimensioni del file attraverso strumenti di compressione, ovvero spezzando il file in più file.
c) Si invitano gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo di prestare molta attenzione nella selezione dei destinatari.
d) Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta. Una quantità troppo elevata di e-mail nella cartella predefinita di arrivo della nuova posta può compromettere sensibilmente la stabilità del programma di posta.
e) Gli utenti devono sempre indicare con chiarezza nel campo oggetto, l'argomento del proprio messaggio. E' possibile richiedere una ricevuta di corretto ricevimento della propria mail. A tale ricevuta va tuttavia assegnata un'importanza relativa poiché talvolta la conferma della ricezione avviene per opera del mail server centrale e non del destinatario ultimo del messaggio.
f) Gli utenti sono invitati a segnalare all'Ufficio Sistemi Informativi aziendale l'arrivo sistematico di messaggi non sollecitati (spam) da determinati indirizzi e-mail.
g) L'attendibilità dell'identità del mittente è molto limitata nella comunicazione via e-mail. E' relativamente facile, infatti, camuffare il mittente di una e-mail. Si richiede pertanto, ogni qual volta sia necessaria la certezza dell'identità del mittente, di verificarne l'identità con i mezzi appropriati.

Sviluppo dei sistemi informativi

a) La necessità di procedure informatiche per la gestione di sistemi informativi aziendali che non trovino adeguate soluzioni in ambito SISSR va segnalata all'Ufficio del Sistema Informativo, che provvederà, secondo le indicazioni di priorità del piano aziendale annuale e nei limiti delle risorse disponibili, a definire le specifiche di sviluppo e le modalità di realizzazione.

b) In particolare l'uso di procedure informatiche non sviluppate in ambito SISSR che utilizzino la rete telematica aziendale devono essere esplicitamente autorizzate dall'Ufficio del Sistema Informativo.

c) Le richieste di installazione e abilitazione di procedure disponibili in ambito SISSR devono essere inoltrate all'Ufficio del Sistema Informativo (non direttamente a INSIEL) ed accompagnate dall'assenso del responsabile di area richiedente.

Assistenza tecnica

a) Per qualsiasi dubbio riguardante la sicurezza informatica, gli utenti devono fare riferimento esclusivamente all'Insiel.

b) In nessun caso l'utente comunicherà per via e-mail, telefono, fax o altro mezzo di comunicazione non sicuro le proprie password.

c) Per nessuna ragione l'utente dovrà comunicare a terzi le proprie password.

d) Le richieste di recupero dati archiviati sui server aziendali ed erroneamente cancellati vanno indirizzate direttamente all'Ufficio del Sistema Informativo.

e) Le richieste di intervento tecnico per malfunzionamenti dell'hardware (comprese le attrezzature in garanzia) e delle procedure informatiche SISSR devono essere indirizzate secondo le modalità esplicitamente previste dall'AAS 3 e in alcun modo autonomamente gestite da operatori o unità operative aziendali. Tutti gli utenti sono invitati a eseguire semplici operazioni di verifica del funzionamento degli strumenti informatici in uso (connessione prese, alimentazione elettrica, ecc.) prima di attivare chiamate per assistenza tecnica. L'Ufficio del Sistema Informativo ha facoltà di verificare le richieste di intervento tecnico per valutare modalità e motivazioni di chiamata.

Privacy

Tutela della Privacy

a) L'AAS3 tutela il rispetto della privacy nelle comunicazioni elettroniche effettuate con le risorse informatiche aziendali predisponendo un complesso di misure di sicurezza secondo quanto previsto dal D Lgs. 196/03.

b) È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nel presente Testo Unico e nell'informativa "obblighi dei dipendenti/convenzionati " valevoli per tutti gli operatori dell'Azienda.

Accesso ai dati senza previo assenso

L' AAS3 accede, senza previo assenso, alla casella di posta elettronica assegnata all'utente e ad ogni altro dato connesso con la comunicazione elettronica effettuata con le risorse informatiche aziendali, nei soli casi elencati e nelle modalità descritte nei successivi paragrafi:

a) nel caso si verifichino delle situazioni d'emergenza;

b) in tutti i casi in cui l'accesso ai dati sia necessario per tutelare la sicurezza del Sistema Informativo aziendale;

c) in caso di autorizzazione dell'Autorità Giudiziaria;

Modalità di accesso ai dati senza previo assenso

L'accesso senza preventiva comunicazione alla casella di posta elettronica assegnata all'utente e ad ogni altro dato connesso con la comunicazione elettronica effettuata con le risorse informatiche aziendali è consentito solamente al Responsabile del Sistema Informativo Aziendale, dopo aver informato il legale rappresentante dell'AAS3 e nei soli casi elencati nel precedente paragrafo.
Il Responsabile del Sistema Informativo Aziendale annoterà su un apposito registro l'accadimento e le modalità di accesso, provvedendo ad informare l'utente appena possibile. Il Responsabile del Sistema Informativo Aziendale sarà responsabile della custodia e della riservatezza delle informazioni raccolte.

Servizio di accesso a Internet tramite Wi-Fi

L'AAS3 mette a disposizione di ospiti e dipendenti la possibilità di accesso, senza abbonamento e a titolo gratuito, alla rete Internet mediante tecnologia Wi-Fi. Il Servizio è utilizzabile nelle aree appositamente predisposte.

Servizio offerto e modalità di richiesta

Il Servizio può essere utilizzato dall'Utente con proprie apparecchiature portatili (PC, telefonini, smartphone, palmari, ecc) compatibili e dotate di scheda wireless certificata dal marchio Wi-Fi, opportunamente configurate. L'accesso al Servizio è consentito mediante un codice di identificazione Utente (User Name) e una parola chiave (Password), cd. Credenziali di Accesso, la cui scadenza sarà annuale rispetto alle date indicate nell'SMS ricevuto durante l'attivazione.

Ai fini dell'attivazione del Servizio, l'Utente deve indicare su apposito modulo on line i propri dati anagrafici, veritieri ed aggiornati, e numero di telefono mobile con SIM italiana intestata. Le Credenziali di Accesso verranno rilasciate con invio di un SMS alla fine della procedura di registrazione.

Le Credenziali di Accesso sono strettamente personali e non trasferibili e identificano ad ogni fine l'Utente nella fruizione del Servizio.

Responsabilità

L'Utente è responsabile dell'utilizzo del Servizio e della segretezza delle Credenziali di Accesso ed è inoltre responsabile di qualsiasi danno causato dalla perdita o diffusione non autorizzata a terzi delle medesime Credenziali di Accesso.

In caso di uso non autorizzato, furto o smarrimento delle credenziali di accesso l'utente deve darne comunicazione tempestiva chiamando il numero telefonico **0432 989352** corrispondente all'ufficio del responsabile sistema informativo aziendale.

Con la consegna delle Credenziali d'Accesso a Internet l'Utente si dichiara al corrente che la AAS3 adotta le misure minime, necessarie e idonee affinché i dati registrati relativi alla data ed ora della comunicazione e alla tipologia del Servizio utilizzato siano mantenuti, con modalità che ne garantiscano l'inalterabilità e la non accessibilità da parte di persone non autorizzate.

L'Utente riconosce espressamente che il Servizio non prevede alcun sistema informatizzato o meno di filtro o controllo sui contenuti visionati, espressi o pubblicati in Rete, e pertanto l'Utente si assume ogni responsabilità in proposito, manlevando e tenendo indenne la ASS3 da ogni pretesa, azione o eccezione che dovesse essere fatta

valere nei suoi confronti da qualsivoglia terzo e/o Autorità di riferimento con riferimento alla messa in uso o fruizione del Servizio.

Ogni utilizzo delle Credenziali a fini illeciti verrà segnalato all'autorità giudiziaria competente. Ogni tentativo intenzionale di forzare o violare i server, l'infrastruttura di rete o i sistemi di autenticazione, con lo scopo di sabotare o impossessarsi dei dati in essa contenuti, danneggiare banche dati o sistemi informatizzati comporterà la denuncia all'autorità giudiziaria.

L'Utente è consapevole del fatto che il Servizio è destinato esclusivamente ad un utilizzo personale e non commerciale ed è obbligato ad utilizzare il Servizio in conformità a tutte le leggi e ai regolamenti vigenti e nel rispetto dei diritti dei terzi. L'Utente prende inoltre atto del fatto che è vietato servirsi o dar modo ad altri di utilizzare il Servizio contro la morale e l'ordine pubblico o con lo scopo di recare molestia alla quiete pubblica o privata, di recare offesa, o danno diretto o indiretto a chicchessia e di tentare di violare comunque il segreto dei messaggi privati.

L'Utente si impegna a non consentire l'utilizzo (anche parziale) a qualunque titolo del Servizio a soggetti terzi. L'Utente sarà responsabile di ogni danno derivante dall'utilizzo delle sue credenziali da parte di terzi.

L'Utente accetta di manlevare e tenere indenne da ogni perdita, danno, responsabilità, costo, spese, incluse anche le spese legali, la AAS3, i suoi dirigenti o impiegati, nei confronti di qualsiasi rivendicazione avanzata da terzi in relazione:

1. all'utilizzo delle Credenziali d'Accesso a Internet da parte dell'Utente stesso, ai sensi dell'art. 2048 del Codice Civile;
2. alla violazione delle presenti Condizioni Generali di Accesso al Servizio;
3. all'utilizzo delle Credenziali d'Accesso a Internet da parte di terzi;
4. alla violazione di qualsiasi diritto di proprietà intellettuale o industriale ovvero di altri diritti altrui.

In tutti i casi d'inadempimento delle obbligazioni sopra indicate, la ASS3 può negare l'accesso al Servizio ai sensi dell'art. 1456 c.c., fatta salva, in ogni caso, l'azione di rivalsa e risarcimento per i danni subiti.

La AAS3 non è responsabile di qualsivoglia inconveniente dovesse manifestarsi nell'erogazione del Servizio ad essa non direttamente imputabile, e non sarà, altresì, in ogni caso considerata responsabile per qualsiasi danno indiretto o eventualmente occorso all'Utente nella fruizione del Servizio.

La AAS3 si riserva il diritto di sospendere in qualsiasi momento la fornitura del Servizio stesso, senza fornire preavviso.