Regolamento per l'utilizzo dei sistemi informatici, delle Telecomunicazioni fissa e mobile, dei fax e delle fotocopiatrici della società Friuli Venezia Giulia Strade S.p.A. *Policy*.

Sommario

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone FVGS e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa. In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare, conseguentemente, eventuali usi scorretti che possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli articoli 2104 e 2105 del codice civile.
Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, FVGS ha adottato il presente Regolamento interno diretto ad evitare che determinati comportamenti possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. I controlli sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo le dotazioni oggetto del presente regolamento strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale ed il conseguente diritto alla riservatezza ed alla dignità, così come sanciti dallo Statuto dei Lavoratori e dalla normativa, nazionale e comunitaria, applicabile in materia di protezione dei dati personali.
Questo Regolamento viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici e/o telematici da parte dei dipendenti, in particolare alla luce degli obblighi previsti dalla normativa italiana ed europea in materia sotto richiamata, dalle Linee Guida del Garante della Privacy per Posta Elettronica ed Internet – Delib. dd.01/03/2007 e dalla legislazione cogente in materia di responsabilità amministrativa delle persone giuridiche (D.Lgs. 231/01 e s.m.i.) e fornendo informazioni in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.
Considerato inoltre che FVGS, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel presente Regolamento alcune clausole relative alle modalità ed ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.
Si precisa che l'eventuale esercizio del potere disciplinare avverrà garantendo un'adeguata previa pubblicità al Regolamento e nel rispetto delle disposizioni del CCNL e del CCRL applicati e dell'art. 7 L. 300/70 e s.m.i..
Si ricorda infine che dal 2018 FVGS si è dotata di un *Data Protection Officer*, ai sensi degli artt. 37 e ss. GDPR, che provvede, fra le altre cose, all'aggiornamento del presente Regolamento in eventuale collaborazione con altri uffici societari interessati, ed è a disposizione degli utenti per qualsiasi chiarimento e/o necessità all'indirizzo mail dpo@fvgs.it .
A causa dell'emergenza dovuta alla pandemia da Covid-19 la Società ha tempestivamente attivato la possibilità - per i dipendenti che ne facessero richiesta - di lavorare da casa con la modalità c.d. *smart working* ai sensi dell'art. 4, comma 1, lett. a) del D.P.C.M. 01/03/2020.
Premesso un tanto si intendono allegate al presente Regolamento, ad integrazione dello stesso, tutte le circolari emesse e/o emanande da FVGS in conseguenza dell'emergenza di cui sopra e nel permanere della stessa fino al suo termine ufficiale (si precisa che alla data di pubblicazione della presente versione aggiornata sono state emesse le Circolari dalla n. 1 alla n.17). Per quanto alla protezione dei dati personali si ricorda, in specie, di garantire il massimo rispetto dell'art. 8 della Circolare n.02/2020, rubricato Riservatezza e Privacy, riportato anche in calce al prossimo paragrafo.

Fonti e riferimenti normativi

- **D.Lgs. n.196/03** – Codice della Privacy (come modificato dal Decreto di adeguamento della normativa nazionale ai principi del GDPR - D.Lgs. n.101/18)
- **Linee Guida del Garante della Privacy per Posta Elettronica ed Internet** – Del. Garante della privacy n.13 dd.01/03/2007
- **D.Lgs. 231/01 e s.m.i.** – Disciplina della Responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica
- **Regolamento Generale sulla Protezione dei dati UE (GDPR) n.679/2016**
- **Delibera della Giunta Regionale n.377/2017** - Progetto di Assessment di Friuli Venezia Giulia Strade redatto da INSIEL S.p.A. – Autorizzazione all'integrazione del Sistema Integrativo di FVG Strade nel Sistema Informativo regionale
- **D.Lgs. n.101/2018** - Decreto di adeguamento della normativa nazionale ai principi del Regolamento Europeo relativo alla protezione delle persone fisiche riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE Regolamento generale sulla protezione dei dati.
- **Delibera della Giunta Regionale n.1109/2019** – D.Lgs. 285/1992 e successive modifiche e integrazioni (Nuovo Codice della Strada). LR 9/2011, Assessment di Friuli Venezia Giulia Strade: implementazione
- **Provvedimento del Garante della Privacy dd.04/12/2019** in materia di disattivazione dell'utenza di dominio e dell'account di posta elettronica aziendale conseguente alla cessazione del rapporto di lavoro per qualsiasi motivo
- **Delibera della Giunta Regionale n.1985/2021** – Aggiornamento dell'indirizzo di cui alla DGR 377/2017. Piano informatico FVGSTRADE: Autorizzazione alla Convenzione diretta tra Fvg Strade ed Insiel

ARTICOLI DI INTERESSE TRATTI DAL CODICE CIVILE

- **Art. 2104 - Diligenza del prestatore di lavoro**
  Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale.
  Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.
- **Art. 2105 - Obbligo di fedeltà**.
  Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio.
- **Art. 2106 - Sanzioni disciplinari.**
  L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo alla applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione.

ARTICOLI DI INTERESSE TRATTI DAL CCNL ANAS APPLICATO

- **Art. 72 - Doveri del lavoratore**

1) Il dipendente deve svolgere la propria attività con diligenza e spirito di collaborazione osservando le disposizioni normative, il regolamento e il Contratto collettivo Nazionale di Lavoro.
2) Il dipendente deve tenere un contegno disciplinato e rispondente ai doveri inerenti l'espletamento delle proprie mansioni, anteponendo al rispetto delle leggi e l'interesse della Società agli interessi privati ed altrui ed in particolare deve:
   a) svolgere con assiduità, diligenza e tempestività le mansioni a lui assegnate;

b) non utilizzare per vantaggi personali, o di soggetti privati od estranei alla Società, le informazioni di cui disponga o venga a conoscenza per ragioni di servizio;
c) astenersi dallo svolgere qualsiasi attività anche a titolo gratuito o qualunque altra forma di partecipazione in imprese che abbiano rapporti con la Società;
d) astenersi dallo svolgere attività contrarie alle finalità della Società o comunque non compatibili con i doveri del proprio ufficio;
e) astenersi dall'utilizzare mezzi o strumenti di lavoro al di fuori delle esigenze di servizio o per fini personali;
f) rispettare l'orario di lavoro, adempiendo alle finalità previste per la rilevazione della presenza, non assentandosi dal luogo di lavoro senza autorizzazione;
g) mantenere, durante l'orario di lavoro, nei rapporti interpersonali con gli utenti, una condotta improntata ai principi di correttezza ed astenersi da comportamenti lesivi della dignità della persona;
h) astenersi dallo svolgere occupazioni estranee al servizio in periodi di malattia o infortunio;
i) avere cura dei locali, mobili, oggetti, macchinari, attrezzature, indumenti, strumenti ed automezzi a lui affidati;
j) non chiedere né accettare a qualsiasi titolo, neanche in occasione di festività, compensi, regali o altre utilità in connessione con la prestazione lavorativa;
k) comunicare alla Società eventuali propri conflitti di interesse;
l) osservare, con scrupolo e diligenza, le disposizioni che regolano l'accesso ai locali della Società da parte del personale e di non introdurre estranei, salvo che non siano espressamente autorizzati, nei locali aperti al pubblico;
m) comunicare alla Società la propria residenza e, ove non coincidente con la sede lavorativa, la dimora temporanea, nonché ogni successivo mutamento delle stesse;
n) non frequentare abitualmente persone o rappresentanti di imprese o di altre organizzazioni che abbiano in corso, presso l'ufficio di servizio, procedimenti contenziosi o volti ad ottenere sovvenzioni, pagamenti, contributi o vantaggi economici di qualsiasi genere;
o) mantenere nelle attività che comportino contatto con il pubblico, un contegno corretto e decoroso al fine di stabilire un rapporto di fiducia e collaborazione con l'utenza;
p) comunicare l'avvenuta notifica dell'informazione di garanzia ricevuta ai sensi dell'art. 70 del presente contratto.

ARTICOLI DI INTERESSE DELLA L. n.300 DEL 20 MAGGIO 1970 C.D. STATUTO DEI LAVORATORI

- **Art. 4 - Impianti audiovisivi e altri strumenti di controllo**

1) Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.
2) La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3) Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

- **Art. 7 - Sanzioni disciplinari**

Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano.
Il datore di lavoro non può adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.
Il lavoratore potrà farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato.
Fermo restando quanto disposto dalla legge 15 luglio 1966, n.604, non possono essere disposte sanzioni disciplinari che comportino mutamenti definitivi del rapporto di lavoro; inoltre la multa non può essere disposta per un importo superiore a quattro ore della retribuzione base e la sospensione dal servizio e dalla retribuzione per più di dieci giorni.
In ogni caso, i provvedimenti disciplinari più gravi del rimprovero verbale, non possono essere applicati prima che siano trascorsi cinque giorni dalla contestazione per iscritto del fatto che vi ha dato causa.
Salvo analoghe procedure previste dai contratti collettivi di lavoro e ferma restando la facoltà di adire l'autorità giudiziaria, il lavoratore al quale sia stata applicata una sanzione disciplinare può promuovere, nei venti giorni successivi, anche per mezzo dell'associazione alla quale sia iscritto ovvero conferisca mandato, la costituzione, tramite l'ufficio provinciale del lavoro e della massima occupazione, di un collegio di conciliazione ed arbitrato, composto da un rappresentante di ciascuna delle parti e da un terzo membro scelto di comune accordo o, in difetto di accordo, nominato dal direttore dell'ufficio del lavoro. La sanzione disciplinare resta sospesa fino alla pronuncia da parte del collegio.
Qualora il datore di lavoro non provveda, entro dieci giorni dall'invito rivoltogli dall'ufficio del lavoro, a nominare il proprio rappresentante in seno al collegio di cui al comma precedente, la sanzione disciplinare non ha effetto. Se il datore di lavoro adisce l'autorità giudiziaria, la sanzione disciplinare resta sospesa fino alla definizione del giudizio.
Non può tenersi conto ad alcun effetto delle sanzioni disciplinari decorsi due anni dalla loro applicazione.

ARTICOLI DI INTERESSE DALLA DELIBERA DEL GARANTE DELLA PRIVACY N.13 DEL 5 MARZO 2013 LINEE GUIDA DEL GARANTE DELLA PRIVACY PER POSTA ELETTRONICA ED INTERNET

TUTTO CIÒ PREMESSO IL GARANTE

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;
2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:
   a) l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);
   b) l'adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:
      si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;

si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;

c) l'adozione di misure di tipo tecnologico, e segnatamente:
   I. rispetto alla "navigazione" in Internet (punto 5.2., a):
   l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
   la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
   il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
   l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
   la graduazione dei controlli (punto 6.1.);
   II. rispetto all'utilizzo della posta elettronica (punto 5.2., b):
   la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
   l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
   la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
   consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
   l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
   la graduazione dei controlli (punto 6.1.);

3) vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:
   a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
   b) la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
   c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
   d) l'analisi occulta di computer portatili affidati in uso;
4) individua, ai sensi dell'art. 24, comma 1, lett. g), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;
5) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

ARTICOLI DI INTERESSE TRATTI DAL GDPR - REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI UE (GDPR) N.679/2016

CAPO IV - Titolare del trattamento e responsabile del trattamento
Sezione 4
Responsabile della protezione dei dati
Articolo 37
Designazione del responsabile della protezione dei dati (Considerando 97)

1) Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
   a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
   b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
2) Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.
3) Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
4) Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.
5) Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
6) Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
7) Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Articolo 38
Posizione del responsabile della protezione dei dati (Considerando 97)

1) Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2) Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3) Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

4) Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
5) Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6) Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39
Compiti del responsabile della protezione dei dati (Considerando 97)

1) Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
   a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
   b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
   d) cooperare con l'autorità di controllo; e
   e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2) Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Conclusioni del Provvedimento del Garante della Privacy dd.04/12/2019 in materia di disattivazione dell'utenza di dominio e dell'*account* di posta elettronica aziendale conseguente alla cessazione del rapporto di lavoro per qualsiasi motivo

TUTTO CIÒ PREMESSO

ai sensi dell'art. 57, par. 1, lett. f) e 58, par. 2, lett. b) del Regolamento, **dichiara illecito il trattamento descritto nei termini di cui in motivazione, consistente nella persistente attività dell'*account* aziendale individualizzato per un ampio periodo di tempo dopo l'interruzione del rapporto di lavoro, con contestuale accesso ai messaggi ivi pervenuti,** ed ammonisce (*omissis*) sulla necessità di conformare i trattamenti effettuati sugli *account* di posta elettronica aziendale dopo la cessazione del rapporto di lavoro alle disposizioni ed ai principi in materia di protezione dei dati personali indicati in motivazione.

Circolare FVGS n.02/2020 – Art. 4 DPCM 01/03/2020 Smart Working
8 - Riservatezza e Privacy

Le rammentiamo, infine, che a norma di legge e di contratto, Lei è tenuto alla più assoluta riservatezza sui dati e sulle informazioni aziendali in suo possesso e/o disponibili sul sistema informativo aziendale e che conseguentemente dovrà adottare –in relazione alla particolare modalità della Sua prestazione ogni provvedimento idoneo a garantire tale riservatezza.
Inoltre, nella qualità di incaricato del trattamento dei dati personali, anche presso il Suo luogo di prestazione fuori sede, dovrà osservare tutte le istruzioni e misure di sicurezza di cui alla lettera di nomina di cui ha già preso visione.
In particolare, con riferimento alla modalità *smart working*, richiamiamo la sua attenzione sui seguenti punti di cui alle citate istruzioni:

- deve porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel suo luogo di prestazione fuori sede;
- deve procedere a bloccare l'elaboratore in dotazione in caso di allontanamento dalla Sua postazione di lavoro anche per un intervallo molto limitato di tempo;
- alla conclusione della prestazione lavorativa giornaliera è obbligatorio da parte Sua conservare e tutelare i documenti eventualmente stampati provvedendo alla loro eventuale distruzione solo una volta rientrato presso la Sua abituale sede di lavoro;
- qualora, invece, in via d'eccezione, al termine del lavoro risulti necessario trattenere presso il Suo domicilio materiale cartaceo contenente dati personali, lo stesso dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura.

1) Entrata in vigore del Regolamento e pubblicità

1.1 Il nuovo Regolamento entrerà in vigore alla data di approvazione. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.2 Copia del Regolamento, oltre ad essere affisso nella bacheca aziendale e pubblicato nella pagina Intranet del DPO, sarà consegnato in fase di formazione introduttiva ai neoassunti. Un avviso degli eventuali aggiornamenti verrà tempestivamente inviato via *mail* a tutti i dipendenti.

1.3 Il Regolamento ha lo scopo di **informare gli interessati anche sulle eventuali finalità e modalità del controllo e sulle specifiche tecnologie adottate per effettuarlo**, in particolare qualora, mediante l'individuazione dei contenuti dei siti visitati, determini un trattamento di dati sensibili per i quali va sempre rispettato il principio dell'indispensabilità.

2) Campo di applicazione del Regolamento

2.1 Il nuovo Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto o in *stage*, ecc.).

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "**utente**" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in *stage*, agente, ecc.) in possesso di specifiche credenziali di autenticazione.

3) Utilizzo del Personal Computer

3.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, nonché violare quanto prescritto dall'art. 617- *quinquies* c.p. e dal d.lgs. 231/01 e s.m.i.. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete di FVGS solo attraverso specifiche **credenziali di autenticazione**, come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 FVGS rende noto che il personale incaricato che opera presso l'Ufficio Sistemi Informatici e Telecomunicazioni della stessa FVGS è autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione *hardware* etc.). Detti interventi, in considerazione dei divieti di cui (ad esempio) ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla

navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'utente e non sia possibile procedere altrimenti.

3.4 Il personale incaricato dell'Ufficio Sistemi Informatici e Telecomunicazioni ha la facoltà di collegarsi e visualizzare in remoto il *desktop* delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, *spyware*, *malware*, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale dell'Ufficio Sistemi Informatici e Telecomunicazioni per conto di FVGS, né agli utenti è consentita l'installazione in via autonoma programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone anche la stessa FVGS a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul *software* (che impone l'utilizzo di *software* regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore) vengono sanzionate anche penalmente.

3.6 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni nel caso in cui siano rilevati virus ed adottando quanto previsto dal punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.7 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito. Si raccomanda pertanto di utilizzare lo *screensaver* a tempo con obbligo di reintrodurre le credenziali per lo sblocco del terminale.

4) Gestione ed assegnazione delle credenziali autentificate

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale dell'Ufficio Sistemi Informatici e Telecomunicazioni, previa formale richiesta del Responsabile dell'ufficio/divisione nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal Responsabile dell'ufficio/ divisione con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (**user id**), assegnato dall'Ufficio Sistemi Informatici e Telecomunicazioni, associato ad una parola chiave (**password**) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Ufficio Sistemi Informatici e Telecomunicazioni.

4.3 La parola chiave, formata da lettere, sia maiuscole che minuscole, numeri e/o caratteri speciali, in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4.4 L'utente incaricato del trattamento al primo utilizzo deve procedere alla modifica della parola chiave; successivamente deve rinnovarla almeno ogni 90 gg.

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni.

4.6 Soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato dell'Ufficio Sistemi Informatici e Telecomunicazioni di FVGS.

4.7 È assolutamente vietata, e punita ai sensi dell'art. 615 quater c.p. al ricorrere delle condizioni di legge, la detenzione abusiva, la diffusione e l'indebita appropriazione di credenziali di autenticazione.

4-bis) Badge per la rilevazione delle presenze e per la guida dei veicoli aziendali

4-bis.1 All'atto dell'assunzione viene consegnato al dipendente un *badge* identificativo (contenente nome, cognome e fotografia dell'interessato), necessario per la rilevazione delle presenze, nonché per la guida dei veicoli aziendali, ai sensi dei protocolli aziendali in tema.

4-bis.2 Detto *badge* è strettamente personale e deve essere custodito con cura, alla pari di tutti gli strumenti consegnati dall'azienda per lo svolgimento della prestazione lavorativa; inoltre, va utilizzato esclusivamente dal dipendente ivi identificato.

4-bis.3 L'eventuale smarrimento deve essere segnalato tempestivamente all'UO Risorse Umane; alla cessazione del rapporto di lavoro, a prescindere dalla motivazione della stessa, deve essere altresì restituito a detto ufficio.

4-bis.4 Al massimo entro un mese dalla cessazione del rapporto di lavoro, il *badge* viene distrutto in maniera protetta, ossia senza illecita diffusione di dati personali, dall'UO Risorse Umane e/o dal DPO; dell'effettiva distruzione deve essere presa apposita nota nel fascicolo personale del dipendente cessato.

4-bis.5 Qualora *badge* validi e funzionanti, correlati a dipendenti in servizio, debbano essere conservati dall'UO Risorse Umane per qualsiasi motivo e per un tempo limitato (per esempio, nelle more della consegna al dipendente in attesa di prendere servizio), devono essere conservati nella cassaforte a disposizione di detto ufficio o comunque in altro luogo dotato di chiave.

5) Utilizzo della rete di FVGS

5.1 Per l'accesso alla rete di FVGS ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3 Le cartelle utenti presenti nei server di FVGS 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. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale dell'Ufficio Sistemi Informatici e Telecomunicazioni. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) **non sono soggette a salvataggio** da parte del personale incaricato dell'Ufficio Sistemi Informatici e Telecomunicazioni. **La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.**

5.4 Il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

5.5 **Con regolare periodicità (almeno ogni tre mesi), ciascun utente deve provvedere alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili; particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.**

6) Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti *know-how* aziendale, devono essere trattati con particolare cautela onde

evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni e seguire le istruzioni da questo impartite. Per poter riutilizzare i supporti di memorizzazione di dati si deve procedere alla cancellazione dei dati precedentemente registrati, in modo da evitare che soggetti terzi possano conoscere o comunque risalire alle informazioni memorizzate in precedenza.

6.3 In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

6.4 L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

6.5 È assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

7) Utilizzo di PC portatili

7.1 L'utente è responsabile del PC portatile assegnatogli dall'Ufficio Sistemi Informatici e Telecomunicazioni e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 Ai PC portatili si applicano le regole di utilizzo previste dal presente Regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

7.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

8) Uso della posta elettronica

8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro di proprietà aziendale concesso in uso al lavoratore al fine di un più proficuo svolgimento della prestazione.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dalla Società; ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile. È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno della Società, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica su dominio **@fvgs.it** per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio di messaggi personali o per la partecipazione a dibattiti, aste *on line*, concorsi, forum o *mailing-list*;
- la partecipazione a catene telematiche (o di Sant'Antonio); non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

8.4 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, PEC), devono essere autorizzate e firmate dalla Direzione Generale, dai Direttori delle Divisioni e/o dai Responsabili di ufficio competenti, a seconda del loro contenuto e dei destinatari delle stesse.

8.5 È obbligatorio porre la massima attenzione nell'aprire i *file attachments* di posta elettronica prima del loro utilizzo (non eseguire *download* di *file* eseguibili o documenti da siti Web o Ftp non conosciuti).

8.6 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. **In tal caso, la funzionalità deve essere attivata dall'utente.** Come previsto dalle Linee Guida del Garante in materia, in previsione che in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato potrà delegare un altro lavoratore (**fiduciario**) a verificare il contenuto dei messaggi e a inoltrare a chi di dovere quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa affidandogli, in modalità protetta, la password del proprio personal computer.

8.7 In caso di assenza non programmata (dovuta ad esempio a "malattia"), qualora non sia possibile acquisire ordinariamente informazioni o comunicazioni che, se non ricevute o recepite con ritardo, potrebbero arrecare un evidente danno alla società, e nel caso non sia stato nominato il fiduciario di cui al punto precedente, sarà consentito al superiore gerarchico dell'utente, tramite il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni e previa informativa al DPO, di accedere alla casella di posta elettronica dell'utente **per ogni ipotesi in cui si renda necessario e non sia possibile procedere altrimenti** cambiando la *password* e informando il lavoratore interessato alla prima occasione utile. Quest'ultimo accesso, analogamente a quello regolato dall'art. 8.7, deve essere formalmente motivato e sottoscritto dal superiore gerarchico. Il provvedimento di cui sopra e il verbale a rappresentazione delle operazioni eseguite sono poi inviati via mail al lavoratore interessato e per conoscenza al DPO.

8.8 Il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3 (cioè garantire la sicurezza e la salvaguardia del sistema, nonché per motivi tecnici e/o manutentivi), previa informativa via mail al DPO.

8.9 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi contengono un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato della FVGS potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale.

8.10 La casella di posta elettronica intestata alle sigle sindacali non è soggetta all'accesso da parte di utenti diversi da quelli autorizzati dal responsabile sindacale, in quanto, ai sensi dell'art. 25 della L. 300/70 e s.m.i., è considerata spazio assimilato alla bacheca sindacale. Lo strumento è finalizzato alla trasmissione di informazioni agli associati o, in generale, al personale dell'azienda, purché i messaggi veicolati siano privi di contenuti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

9) Navigazione in Internet

9.1 **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa e durante l'attività stessa. Al di fuori dei tempi di lavoro nei modi constatabili attraverso il rilevatore automatico di presenze (ad esempio durante la pausa pranzo), è eccezionalmente consentito all'utente di accedere ad internet per visionare la propria casella di posta elettronica personale e/o siti non vietati (c.d. *black list*), purché ciò non comporti il rischio di compromissione del sistema (virus, etc.). Il dipendente è comunque responsabile di eventi dannosi determinati a seguito dell'esercizio di quest'ultima facoltà.

9.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:

- *l'upload* o il *download* di *software* gratuiti (*freeware*) e *shareware*, nonché l'utilizzo di documenti provenienti da siti *web* o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di *remote banking*, acquisti *on-line* e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale o dall'Amministratore Delegato (ad esempio Area Amministrazione e Finanza);
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa; la partecipazione a Forum non professionali, l'utilizzo di *chat line*, di *social networks*, di bacheche elettroniche e le registrazioni in *guest books* anche utilizzando pseudonimi (o *nicknames*) se non espressamente autorizzati dal Responsabile d'ufficio;
- accesso, tramite internet, a caselle *webmail* di posta elettronica personale durante l'orario di lavoro.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, FVGS rende nota l'avvenuta adozione di uno specifico sistema di blocco o filtro automatico che previene l'accesso a determinati siti inseriti in uno specifico elenco connotato dalla non pertinenzialità con l'attività svolta dalla Società (fatto salvo l'eventuale sblocco dell'accesso ad un determinato sito di cui il lavoratore motivi specificamente la necessità o utilità per lo svolgimento delle proprie funzioni lavorative).

A seguito della **Delibera della Giunta Regionale n.377/2017** - *Progetto di Assessment di Friuli Venezia Giulia Strade redatto da INSIEL S.p.A. – Autorizzazione all'integrazione del Sistema Integrativo di FVGStrade nel Sistema Informativo regionale*, la società INSIEL S.p.A. si occupa, fra le altre cose, della configurazione di tale filtro di navigazione e dell'individuazione delle categorie dei siti internet da escludere dalla navigazione; di seguito si riporta l'elenco attuale:

- Siti per adulti, pornografici o sessualmente espliciti
- Pornografia minorile
- Siti di incontri
- Gambling (gioco d'azzardo)
- Hacking (Pirateria informatica)
- Piracy (download illegale di musica, film ecc…)
- Illegal drug (farmaci illegali)
- Illegal software (software illegali)
- Instant Messaging, Chat (sistemi di comunicazione fra pc in tempo reale in rete, es. Messenger)
- Malware (software dannosi usati per disturbare un computer, sottrarre dati sensibili, ecc.)
- Peer to peer (Software che permette di scambiarsi file fra utenti collegati a Internet)
- Radio/audio streaming
- Social networking (es. Facebook, Instagram, ecc.)
- Spam (posta elettronica indesiderata e fastidiosa)
- Suspicious (siti sospetti)
- Violence and Weapons (violenza e armi)
- Proxy avoidance (siti che permettono l'elusione del filtro proxy)

9.4 Nell'utilizzo dei propri *account* di *social media*, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla Società. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine della Società o della PA in generale.

9.5 Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le

comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

9-bis) Disattivazione dell'utenza di dominio e dell'account di posta elettronica aziendale a seguito di cessazione del rapporto di lavoro

9-bis.1 In ossequio al provvedimento del Garante della Privacy dd.04/12/2019 in materia di disattivazione dell'utenza di dominio e dell'*account* di posta elettronica aziendale conseguente alla cessazione del rapporto di lavoro per qualsiasi motivo, **si deve procedere secondo le modalità di seguito descritte.**

9-bis.2 L'UO Risorse Umane informa l'UO Assistenza Informatica, tramite gli usuali canali di comunicazione concordati con gli uffici interessati, della cessazione del rapporto di lavoro in relazione a un determinato dipendente, almeno 7 giorni prima del termine, qualora possibile.

9-bis.3 A seguito di ciò l'UO Assistenza Informatica provvede a:

a) Disattivare l'utenza di dominio;
b) Disabilitare la casella di posta elettronica, in modo che non possa ricevere mail dall'esterno, non possa inviare mail e l'indirizzo non venga visualizzato nella rubrica aziendale;
c) **Dopo 1 mese dalla comunicazione** eliminare completamente la casella postale con conseguente totale perdita di quanto ivi contenuto;
d) cancellare infine l'utenza di dominio.

9-bis.4 Dell'eliminazione della casella postale e della cancellazione dell'utenza di dominio viene data tempestiva e sintetica comunicazione via mail al DPO.

9-bis.5 Qualora per ragioni contingenti (per esempio poiché devono essere completate le operazioni di trasferimento dei dati di cui il dipendente era in possesso per ragioni di lavoro) fosse necessario ritardare l'eliminazione della casella di posta elettronica e/o la cancellazione dell'utenza di dominio, il Direttore della Divisione interessata, prima del termine del rapporto di lavoro, **formula apposita richiesta motivata via mail all'UO Assistenza Informatica,** inserendo pc il DPO nella comunicazione.

9-bis.6 Alla cessazione del motivo sopra indicato, comunicata dal Direttore di cui sopra, e comunque non oltre tre mesi dalla comunicazione delle Risorse Umane di cessazione del rapporto di lavoro, l'UO Assistenza Informatica procede all'eliminazione e/o cancellazione della casella postale e dell'utenza di dominio come di norma, informando contestualmente via mail il DPO.

10) Protezione antivirus

10.1 Il sistema informatico di FVGS è protetto da *software* antivirus aggiornato in modo continuativo. **Si ricorda tuttavia che ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro *software* aggressivo.**

10.2 Nel caso il *software* antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer, nonché segnalare prontamente l'accaduto al personale dell'Ufficio Sistemi Informatici e Telecomunicazioni.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale dell'Ufficio Sistemi Informatici e Telecomunicazioni.

11) Utilizzo dei telefoni aziendali

11.1 **Il telefono aziendale fisso affidato all'utente è uno strumento di lavoro.** Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. L'effettuazione di

telefonate personali è consentita solo nel caso di comprovata ed assoluta necessità ed urgenza, con onere di successiva motivata informativa al Responsabile dell'Ufficio Competente.

11.2 Il dipendente cui è assegnato un telefono cellulare aziendale è responsabile del suo utilizzo e della sua custodia. Attualmente i contratti di Telecomunicazioni prevedono delle ricariche automatiche mensili con a disposizione 20GB per i dati, 3000 minuti per le telefonate e 300 SMS e i nuovi telefoni prevedono la possibilità di inserirvi una seconda SIM personale; l'eventuale uso promiscuo del telefono è disciplinato dalle direttive/comunicazioni dell'Ufficio Sistemi Informatici e Telecomunicazioni trasmesse all'uopo a tutti i dipendenti.

11.3 Ciascun Responsabile di Area trasmette alla Direzione Generale apposita richiesta di assegnazione evidenziando il nominativo dell'assegnatario nonché le principali esigenze di utilizzo del telefono cellulare. Per la fornitura di eventuali servizi aggiuntivi di trasmissione dati (schede PCMCIA – Gprs, Edge, Umts con relative SIM Card) la Direzione Generale acquisirà il parere dell'Ufficio Sistemi Informatici e Telecomunicazioni. In caso di cambio mansioni di un dipendente, la Direzione Generale può, valutato il caso concreto e, sentito il nuovo Responsabile, revocare l'assegnazione del telefono aziendale.

11.4 In caso di cessazione del rapporto di lavoro o revoca del terminale, il dipendente (ad esclusione del personale che utilizza il telefono aziendale in modo condiviso) potrà mantenere, a richiesta, l'utilizzo dell'utenza telefonica mobile. In questo caso l'Ufficio Sistemi Informatici e Telecomunicazioni predisporrà la documentazione necessaria affinché il dipendente diventi titolare della SIM. Se il dipendente non ritenesse di volere mantenere la disponibilità dell'utenza assegnata sarà tenuto a restituire con la massima tempestività all'Ufficio Sistemi Informatici e Telecomunicazioni la SIM e l'apparato radiomobile fornito, completo di eventuali accessori.

11.5 Il *backup* dei dati contenuti sul telefono aziendale è sempre e comunque a carico del dipendente.

11.6 **Ferme eventuali responsabilità personali,** la Società si riserva, qualora risultino sussistere problematiche inerenti l'utilizzo del telefono aziendale, sia fisso che mobile, di informare preventivamente il possessore del telefono o del telefonino tali problematiche, affinché possa verificare e, se possibile, porre fine alle stesse. Nel caso le stesse perdurino, potranno essere avviati esami dei tabulati telefonici e della navigazione *internet*, dovendosi un tanto intendersi quale "controllo difensivo" atto cioè a tutelare esclusivamente l'impiego di un bene aziendale e i costi a ciò relativi. Di quest'ultima attività sarà data notizia ai Dirigenti o Responsabili competenti.

11.7 Per quanto riguarda il personale operativo su strada, si precisa che il telefono cellulare con la relativa utenza è assegnato a fini esclusivamente lavorativi alla squadra nella sua totalità; viene detenuto e utilizzato dal **Capo Squadra** in quanto persona di riferimento della stessa, non come uno strumento personale; in caso di assenza del Capo squadra, pertanto, il telefonino deve essere preso in consegna e utilizzato da un altro componente della squadra, designato dal Capo Nucleo e/o dal Capo Centro. Le *app* di messaggistica istantanea, quali ad esempio Whatsapp, possono essere legittimamente utilizzate a fini lavorativi per la trasmissione di dati e informazioni, immagini comprese, fra i membri della squadra e/o il resto del personale della Società.

12) Utilizzo dei fax e delle fotocopiatrici aziendali

12.1 È vietato l'utilizzo dei fax e delle fotocopiatrici aziendali per fini personali, salvo preventiva, eccezionale ed esplicita autorizzazione da parte del Responsabile di ufficio.

12.2 A fine 2019 sono state installate, su disposizione della RAFVG con l'apporto di INSIEL e dell'impresa Iscopy, nuove multifunzioni il cui utilizzo avviene esclusivamente tramite *badge* aziendale fatto scorrere nel lettore installato a fianco della multifunzione). A seguito di verifica con il DPO di INSIEL è risultato che queste multifunzioni trattano esclusivamente i numeri del *badge* del personale dipendente (ovvero dati pseudonimizzati che non permettono l'immediata identificabilità dell'utente.

12.3 Nell'utilizzare stampanti poste al di fuori della propria postazione lavorativa, diverse da quelle di cui al paragrafo precedente, è opportuno assicurare una tempestiva acquisizione dei documenti al fine di evitare l'accesso di persone non autorizzate agli stessi.

12.4 Per quanto riguarda l'invio di fax, di recente la RAFVG ha messo a disposizione di FVG Strade un servizio di *fax server* che converte i fax in arrivo sulle numerazioni aziendali in *e-mail* poi inoltrate alle relative caselle di posta elettronica aziendali.

L'operazione d'invio di un fax è simile a quella dell'invio di una normale mail tramite l'interfaccia di Microsoft Outlook. È sufficiente, quindi, generare un nuovo messaggio di posta elettronica ed indicare, nel campo "A", il numero di fax del destinatario, rispettando il seguente il formato:

numero-fax@faxtrieste.regione.fvg.it

Il documento da spedire funge da allegato a questa mail, pertanto è obbligatorio inserire nel documento un frontespizio per indicare il mittente, il numero di fax del mittente (per la ricezione di eventuali risposte) e l'oggetto del documento. Il "corpo" della mail non deve contenere alcun testo in quanto, in caso contrario, assieme al documento allegato verrebbe generata e inviata anche una pagina iniziale generica che non contiene alcuna informazione specifica.
Nell'utilizzo del Fax occorre controllare l'esattezza del numero di telefono inserito prima di inviare il documento e attendere la mail contenente il rapporto di trasmissione per una verifica dell'esattezza della stessa.

13) Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di trattamento dei dati personali, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi della normativa vigente.

14) Accesso ai dati trattati dall'utente

14.1 E' facoltà della Direzione Generale, tramite il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni e previa informativa al DPO al fine della verifica del rispetto della normativa sulla privacy, accedere, a dati trattati dall'utente, preventivamente informato, salvo quanto previsto al punto 8.11, oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.), motivazioni comunque estranee a qualsiasi finalità di controllo dell'attività lavorativa.

14.2 In adempimento alla normativa vigente i dati acquisiti per il tramite delle attività sub 14.1 sono trattati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti e non potranno essere utilizzati come elementi atti a istituire provvedimenti disciplinari e risarcitori previsti dal CCNL applicato, nonché per eventuali azioni civili e penali.

14.3 La conservazione del tracciato riguardante le pagine visitate (*log*) viene conservato per un massimo di 15 giorni, per finalità organizzative, di sicurezza e di verifica delle funzionalità del sistema di protezione. Trascorso tale periodo, il sistema cancellerà in modo automatico tali tracciati.

14.4 I trattamenti connessi al servizio Proxy sono curati solo da INSIEL S.p.A.. Nessun dato derivante dal servizio PROXY può essere comunicato o diffuso, salvo nei casi previsti dalla legge.

15) Sistemi di controlli graduali

15.1 In caso di anomalie, il personale incaricato dell'Ufficio Sistemi Informatici e Telecomunicazioni, previa preventiva informazione all'area di riferimento della stessa, potrà effettuare controlli anonimi che si concluderanno con un avviso generalizzato diretto ai dipendenti del settore in cui è stata rilevata la criticità, nel quale si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad

attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Perdurando la situazione anomala tali controlli, nelle forme e per le motivazioni di cui sopra, potranno essere effettuati su base individuale, nel rispetto della normativa che vieta controlli prolungati, costanti o indiscriminati; all'esito degli stessi potrà essere avviato, nei confronti del dipendente interessato, regolare procedimento disciplinare nelle forme e nei modi di cui alla legge ed al CCNL applicato.

16) Sanzioni

16.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra richiamate, qualora siano ravvisabili profili quantomeno colposi nella condotta osservata, è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari e risarcitori previsti dal CCNL applicato.

16.2 Si ammonisce, altresì, il dipendente a non intercettare, interrompere o impedire le comunicazioni informatiche/telematiche (art. 617 *quater* c.p.) e a non danneggiare informazioni, dati o programmi informativi nonché i sistemi informatici o telematici aziendali e/o di pubblica utilità (artt. 615 *quinquies* c.p., 635 *bis* c.p., 635 *ter* c.p., 635 *quater* e 635 *quinquies* c.p.).

17) Aggiornamento e revisione

17.1 La presente versione del Regolamento, preliminarmente inviata alle OO.SS. in data 04/09/2022, è stata approvata dal Titolare del Trattamento con dispositivo prot. n.2109 dd.19/09/2023.