REGOLAMENTO INTERNO SULL'UTILIZZO DEL SISTEMA E DEGLI STRUMENTI INFORMATICI AZIENDALI

1. INTRODUZIONE

1.1 Premesse

Con il presente documento, SANVIGO SRL, Titolare del trattamento dei dati personali (per brevità d'ora innanzi "Titolare" o "la società"), intende definire e regolare le modalità d'uso del sistema e degli strumenti informatici aziendali, e, in particolare, di posta elettronica ed internet, da parte di dipendenti e collaboratori che, per ragioni di servizio, abbiano ricevuto in dotazione un personal computer o dispositivi analoghi (ad esempio tablet e smartphone) ovvero, in ogni caso, abbiano accesso a strumenti informatici e telematici. È, infatti, indiscutibile l'esigenza del datore di lavoro di assicurare la funzionalità ed il corretto impiego dei sistemi informatici aziendali, ed in particolare di posta elettronica e rete internet, da parte dei propri lavoratori, e di adottare, quindi, idonee misure di sicurezza atte a prevenirne utilizzi indebiti, e ciò in ragione di imprescindibili esigenze organizzative e di sicurezza. È, peraltro, necessario che ciò avvenga nel rispetto dei diritti dei lavoratori medesimi, con particolare riguardo al profilo del corretto trattamento dei dati personali che il datore può acquisire in conseguenza dell'utilizzo degli strumenti informatici aziendali da parte dei propri dipendenti e dei propri collaboratori. Con proprio Provvedimento Generale del 01.03.2007, il Garante per la Protezione dei dati personali ha, dunque, indicato ai datori di lavoro alcune linee guida, l'adeguamento alle quali dovrebbe garantire il bilanciamento delle contrapposte esigenze di cui sopra.

1.2 Scopo e campo di applicazione

Nell'ambito, dunque, delle proprie responsabilità, SANVIGO SRL ha provveduto a redigere ed emanare il presente Regolamento, che si compone di due parti. Vengono, anzitutto, delineate le regole che costituiscono il disciplinare interno per un corretto uso degli strumenti informatici aziendali (personal computer e simili, posta elettronica aziendale, internet, rete aziendale), alle quali tutti i dipendenti, collaboratori e agenti, sono tenuti a conformarsi. Nella seconda parte del Regolamento la società intende informare i propri dipendenti/collaboratori delle procedure adottate dalla propria organizzazione, finalizzate a garantire un corretto e regolare svolgimento dell'attività di impresa nell'ipotesi in cui si rendesse necessario accedere ad informazioni contenute nella casella di posta elettronica aziendale assegnata al singolo dipendente/collaboratore, ovvero svolgere attività di manutenzione del sistema; in secondo luogo, in ottemperanza ai principi di correttezza e di proporzionalità invocati nel Provvedimento sopra richiamato, vengono esplicitate le modalità con le quali il datore di lavoro potrà svolgere un controllo sull'utilizzo del sistema informativo aziendale, nel rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. **L'attenzione ai dati personali che il Titolare garantisce di proteggere ai propri interessati, parte anche dalle scrivanie di lavoro, nel non lasciare incustoditi o alla visione occasionale di eventuali estranei, soprattutto in appuntamenti pianificati, fogli o cartelle con dati personali, anche sensibili in violazione alle Informative predisposte. Le stesse accortezze devono essere intraprese nell'utilizzare fogli "riciclati" contenenti dati personali, di qualsiasi natura, su una delle facciate utilizzate in precedenza e nel non divulgare, nemmeno oralmente, notizie, impressioni, giudizi o elementi di qualsiasi natura che riguardano Clienti, Fornitori, Dipendenti, Candidati e loro cv e altri Collaboratori che formano nel loro insieme gli interessati di cui SANVIGO SRL si impegna alla protezione dei dati personali.**

1.3 Riferimenti normativi

- Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (per brevità, d'ora innanzi anche semplicemente Regolamento UE)
- Decreto Legislativo 30.06.2003 n. 196, Codice in materia di protezione dei dati personali (per brevità, d'ora innanzi anche semplicemente il Codice della Privacy).
- Provvedimento a carattere generale del Garante per la protezione dei dati personali del 01.03.2007, "Lavoro le linee guida del Garante per posta elettronica ed internet" (per brevità, d'ora innanzi anche semplicemente Provvedimento 01.03.2007).
- Provvedimento a carattere generale del Garante per la protezione dei dati personali del 27.11.2008, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e successive modifiche.

2. REGOLE DI UTILIZZO DEL SISTEMA INFORMATIVO AZIENDALE

2.1 Personal computer, tablet e smartphone

2.1.1 Uso del personal computer

Il personal computer (fisso o portatile) affidato al dipendente e/o collaboratore della società costituisce uno strumento di lavoro. Ne consegue che è vietato ogni utilizzo dello stesso non inerente l'attività lavorativa o per finalità estranee al rapporto di lavoro, potendo lo stesso contribuire, in alcuni casi, ad innescare disservizi, costi di manutenzione, minacce alla sicurezza della rete, ecc. Tutti i documenti inerenti l'attività lavorativa prestata dal dipendente o da esso creati nello svolgimento delle proprie mansioni utilizzando dispositivi collegati alla rete locale aziendale, dovranno essere memorizzati nelle unità di rete condivise e, dunque,

SANVIGO S.r.l. - Via Verona 92 - 37068 – Vigasio (VR) - P.Iva 03242850232

accessibili ai responsabili e/o ai dipendenti della società a ciò autorizzati. Il personal computer deve essere custodito con cura, deve avere installati appositi software di sicurezza da mantenere aggiornati e ciascun incaricato dovrà segnalarne tempestivamente all'azienda l'eventuale furto, smarrimento, danneggiamento, ecc. Il personal computer dove essere spento ogni sera prima di lasciare l'ufficio e/o in ogni caso di assenza prolungata dalla propria postazione di lavoro. Qualora sorgesse l'esigenza di assentarsi dalla propria postazione, anche per brevi periodi, ciascun incaricato dovrà attivare, in ogni caso, il blocco del sistema con richiesta di password per la riattivazione, ovvero porre il personal computer in modalità stand-by (facilitazione: combinazione di tasti: logo/bandierina di Windows e lettera L). **Per quanto riguarda l'accesso al gestionale in dotazione, ogni dipendente è obbligato a scollegarsi al termine del proprio turno per consentire la corretta procedura di autenticazione. Nel caso un dipendente trovasse una sessione di lavoro aperta che non gli appartiene, è tenuto a scollegarla ed effettuare in modo corretto il proprio login.**

2.1.2 Gestione delle credenziali di autenticazione

L'accesso a ciascun profilo utente è protetto da una coppia di credenziali di autenticazione (nome utente e password), che permettono al sistema di verificare l'identità di colui che sta tentando l'accesso. Le credenziali di autenticazione assegnate a ciascun incaricato devono essere da questi custodite con la massima diligenza e riservatezza. In particolare:

- la password non deve essere scritta su alcun supporto, bensì memorizzata o conservata in luogo separato e protetto e non deve mai essere comunicata a terzi, per alcuna ragione;
- la password deve essere cambiata ogni 6 mesi (3 mesi in caso di trattamento di dati sensibili), deve avere una lunghezza minima di 8 caratteri e presentare un certo grado di complessità (ad esempio, non deve corrispondere in nessuna forma, né modificata né integrata da cifre o lettere, al nome dell'utente e non deve contenere riferimenti facilmente riconducibili allo stesso, né parole comuni di senso compiuto, ecc.).

In caso di prolungata assenza o di impedimento dell'incaricato, il Titolare del Trattamento dei Dati Personali, per mezzo di personale interno a ciò incaricato, potrà accedere all'elaboratore, nel rispetto delle procedure e dei criteri che verranno illustrati nel capitolo 3 del presente Regolamento.

2.1.3 Utilizzo di supporti di comunicazione e di memoria esterni

È fatto divieto di installare sul computer in dotazione, dispositivi propri di memorizzazione, comunicazione o altro (quali modem, masterizzatori, HD Drive, ecc.), se non previa autorizzazione espressa dell'azienda.
Tutti i supporti esterni riutilizzabili (CD/DVD, dischetti, cassette, chiavi USB, ecc.) contenenti dati devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la cancellazione e, addirittura, anche dopo la formattazione del supporto stesso.

2.1.4 Installazione di software applicativi

Salva diversa espressa autorizzazione aziendale, è vietato installare autonomamente programmi provenienti dall'esterno, anche se freeware o shareware, in quanto sussiste il concreto pericolo che tali programmi possano contenere software maligni di vario genere. E', altresì, vietato l'uso di programmi diversi da quelli distribuiti, installati ed autorizzati dalla società. In particolare, è vietato utilizzare programmi non distribuiti ufficialmente e/o non dotati di regolare licenza d'uso. L'inosservanza delle disposizioni che precedono, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la società a responsabilità civile e/o penale, in caso di violazioni della normativa a tutela del diritto d'autore. È vietato effettuare il download e la riproduzione di file musicali e di opere cinematografiche per scopi estranei all'attività lavorativa, anche se dotati della relativa licenza d'uso. Non è consentito all'incaricato di modificare le caratteristiche impostate sul proprio personal nonché le configurazioni del sistema operativo, se non con esplicita autorizzazione da parte del Titolare.

2.1.5 Utilizzo della rete aziendale

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, nessun file che non sia legato all'attività lavorativa potrà essere memorizzato, nemmeno per brevi periodi, in queste unità. È vietato, in ogni caso, memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione ed appartenenza sindacale e/o politica. È, parimenti, vietata la visione e/o l'archiviazione di immagini o di contenuti multimediali a carattere osceno, riservati ad un pubblico adulto o, comunque, tali da offendere il comune senso del pudore. Le password di accesso alla rete ed ai programmi sono segrete e vanno gestite secondo le procedure sopra illustrate. È vietato accedere alla rete ed ai programmi autenticandosi con credenziali altrui. L'azienda si riserva la facoltà di procedere, in qualunque momento, alla rimozione di ogni file e/o applicazione che dovesse ritenere pericolosi per la

sicurezza dei personal computer in dotazione degli incaricati e/o della rete e, comunque, installati in violazione delle regole sopra descritte. È cura dell'utente effettuare la stampa di dati solo se necessaria e di ritirarla prontamente dai vassoi delle stampanti di uso comune. È opportuno evitare di stampare documenti a carattere strettamente riservato su stampanti comuni. In caso di collegamento alla rete aziendale da remoto, ove possibile, è buona norma evitare applicazioni quali telnet, ftp e X Windows, in quanto le stesse non criptano i dati durante la sessione di collegamento. Pertanto, ove possibile, si devono prediligere applicazioni di tipo SSH (Secure SHell) che invece permettono di stabilire una sessione remota cifrata con un altro host.

2.1.6 Tablet e dispositivi mobili

Le regole che precedono e, in generale, quelle previste dal presente Regolamento, si applicano, in quanto compatibili, anche in relazione ad eventuali dispositivi elettronici diversi dal personal computer, quali tablet, smartphone, ecc., assegnati in uso da parte della società o di proprietà del dipendente/collaboratore.

In particolare, per tali dispositivi è necessario:

- l'uso della password o di codici di sblocco del dispositivo mobile
- l'uso di apposito software antivirus
- l'uso di software di *remote wiping* per cancellare i dati una volta che il dispositivo dovesse cadere in mani sbagliate
- rimuovere tutti i dati aziendali al momento della cessazione del rapporto di collaborazione/lavoro dipendente

2.2 Posta elettronica aziendale

2.2.1 Indicazioni generali per un corretto utilizzo

SANVIGO SRL mette a disposizione dei propri dipendenti/collaboratori indirizzi di posta individuali, condivisi tra più utenti (ad esempio, mario.rossi@montemezzi.it). **La posta elettronica è, in ogni caso, un bene aziendale**. Ciascun messaggio inviato dalla casella di posta elettronica aziendale individuale deve contenere il seguente avvertimento indirizzato automaticamente ai destinatari, circa la sua natura non privata e circa la possibilità che, nei limiti di legge e secondo le regole di cui al presente Regolamento, al quale si rinvia, la società SANVIGO SRL venga a conoscenza dei messaggi inoltrati dal ed al predetto indirizzo:

Le informazioni, i dati e le notizie contenute nella presente comunicazione e i relativi allegati sono di natura privata, riservata e inviate esclusivamente ai destinatari indicati. La diffusione, distribuzione e/o la copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p., sia ai sensi del D.Lgs. n. 196/2003 e del Regolamento UE 679/2016. Se avete ricevuto questo messaggio per errore, vi preghiamo di distruggerlo e di darcene immediata comunicazione anche inviando un messaggio di ritorno all'indirizzo e-mail del mittente. Si evidenzia altresì che, essendo la presente casella di posta elettronica di uso aziendale, il suo monitoraggio può non essere esclusivamente riservato ad un solo incaricato; si invita pertanto a considerare questo aspetto per le eventuali risposte.

Ciascun incaricato che ha facoltà di utilizzare l'indirizzo di posta elettronica aziendale (sia esso di uso individuale o condiviso) è responsabile del corretto utilizzo della stessa nonché della custodia della credenziale di autenticazione necessaria all'accesso alla predetta. È vietato, quindi: 1) utilizzare la posta elettronica aziendale per motivi non attinenti allo svolgimento delle proprie mansioni, ad esempio, per l'invio o la ricezione di messaggi personali, salva diversa ed espressa autorizzazione; 2) inviare messaggi totalmente estranei al rapporto di lavoro ed alle relazioni tra colleghi; 3) partecipare a dibattiti, forum, mailing-list, blog, social e simili, salva diversa ed espressa autorizzazione; 4) inviare catene telematiche (o di Sant'Antonio), o parteciparvi; nel caso pervenissero messaggi di tale genere, non si dovranno in alcun modo attivare i relativi allegati, e si dovrà immediatamente avvertire il Titolare del trattamento o il servizio di assistenza informatica; 5) leggere messaggi di posta elettronica di provenienza incerta e/o che contengano allegati non ben identificati e/o che presentino un oggetto particolare. I messaggi di spam ricevuti devono essere cancellati immediatamente, non appena ricevuti, senza leggerne il contenuto né aprirne eventuali allegati; 6) inviare e memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione ed appartenenza sindacale e/o politica.

Salvo espressa autorizzazione della società, è vietato l'utilizzo della posta elettronica per l'invio di documenti "strettamente riservati", anche se inerenti l'attività lavorativa, sussistendo il rischio che la posta inviata all'esterno della rete possa essere intercettata da estranei. Ogni comunicazione inviata tramite posta elettronica, che contenga un impegno della società verso terzi, dovrà essere seguita da un successivo invio della medesima attraverso le regole della corrispondenza ordinaria ovvero a mezzo fax o PEC, oppure dovrà essere seguita apposita procedura indicata dal Titolare. La casella di posta elettronica deve essere mantenuta in ordine, cancellando periodicamente documenti inutili, specie se correlati ad allegati "pesanti" in termini di occupazione di memoria. È obbligatorio controllare tutti gli allegati di posta elettronica prima del loro utilizzo, e verificare che non presentino virus o altri codici malevoli.

2.3 Navigazione in internet

2.3.1 Indicazioni generali per un corretto utilizzo della rete internet e dei relativi servizi

La navigazione in internet, alla quale fosse eventualmente abilitato il personal computer o altro dispositivo concesso in uso al singolo incaricato, costituisce uno strumento aziendale funzionale allo svolgimento della propria attività lavorativa del quale l'utente deve fare uso secondo criteri di ragionevolezza e professionalità. È, quindi, vietata la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa, soprattutto in siti idonei a rivelare le opinioni politiche, religiose, sindacali, sanitarie e di orientamento sessuale del lavoratore. In particolare, è vietato/a:
1) effettuare download di file di varia natura e/o di software, anche se freeware o shareware, da siti web e/o da piattaforme peer to peer o simili (quali KaZaA, Bearshare, Edonkey, Emule, BitTorrent, ecc.), salva espressa autorizzazione del Titolare; 2) effettuare ogni genere di transazione finanziaria, ivi comprese operazioni di remote banking, acquisti online e simili, per scopi non attinenti l'attività lavorativa, salvi i casi espressamente autorizzati dall'azienda e con il rispetto delle normali procedure di acquisto. È, altresì, vietata ogni forma di registrazione a siti i cui contenuti non siano strettamente attinenti all'attività lavorativa; 3) la partecipazione a forum non professionali e a blog, l'utilizzo di chat-line (esclusi gli strumenti autorizzati), di mailing-list, di bacheche elettroniche, la registrazione in guest book, anche utilizzando pseudonimi (o nicknames) nonché la registrazione o l'accesso a social network (facebook, twitter, ecc.) se non con l'autorizzazione del Titolare. In conformità al principio di necessità e secondo le indicazioni di cui al Provvedimento del 01.03.2007, SANVIGO SRL si riserva la facoltà di introdurre sistemi di filtro che prevengano l'accesso a determinati siti o categorie di siti, dandone informazione ai soggetti interessati.

2.4 Sanzioni

SANVIGO SRL ricorda che la violazione delle regole aziendali in materia di utilizzo dei sistemi informatici potrà comportare l'irrogazione di sanzioni disciplinari, sino a legittimare il licenziamento del lavoratore interessato, salvi eventuali profili di responsabilità civile e/o penale.

3. ACCESSO AI DATI PERSONALI DELL'UTENTE — CONTROLLI DELLA SOCIETÀ SULL'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

3.1 Premessa

Fermo restando che la casella di posta elettronica aziendale condivisa è sempre accessibile a tutti i dipendenti abilitati ad accedervi, evidenti esigenze aziendali connesse al regolare svolgimento dell'attività lavorativa possono rendere necessario l'accesso della società anche ai dati contenuti in eventuali caselle di posta elettronica utilizzate individualmente da propri dipendenti. Esigenze produttive e di salvaguardia del patrimonio e della sicurezza aziendali impongono, altresì, alla società di vigilare sul corretto utilizzo del proprio sistema informativo cui possono accedere, per ragioni di servizio, i propri dipendenti, con potere di reprimere, se necessario, comportamenti o attività contrari alle regole sopra illustrate. Tale attività di controllo da parte della società, che potrà essere effettuata anche in occasione di verifiche sulla funzionalità e la sicurezza del sistema, può portare all'acquisizione di informazioni, anche sensibili, sui lavoratori interessati, e ciò sia in relazione all'utilizzo dei dispositivi elettronici forniti in uso ai dipendenti, sia in relazione all'uso della posta elettronica e della navigazione in internet.

3.2 Manutenzione del sistema - la figura dell'amministratore di sistema

La società si avvale, per la gestione e la manutenzione dei propri strumenti informatici, dell'attività di soggetti terzi, questi ultimi operanti anche a mezzo di propri incaricati. In particolare, ai sensi del Provvedimento Generale del Garante del 27.11.2008 e successive modifiche, tutte le figure professionali finalizzate alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti, in senso ampio, ivi compresi, quindi, coloro che amministrano le basi di dati, ovvero gli amministratori di rete e di apparati di sicurezza, e gli amministratori di sistemi software complessi, rientrano nella categoria dei c.d. "amministratori di sistema". La scrivente società ha richiesto ai soggetti esterni, cui è stato affidato il servizio di amministrazione di sistema, i nominativi delle persone fisiche dagli stessi preposte a tale attività, come previsto dal citato provvedimento. Nell'ambito dei poteri e delle funzioni ad essi specificamente attribuite, gli amministratori di sistema potranno accedere, anche indirettamente, ai sistemi che trattano dati di carattere personale dei lavoratori, ivi compresi i dati registrati dai programmi in uso, relativi ai file di lavoro, al traffico internet e di posta elettronica dei dipendenti/collaboratori. Tale accesso avverrà solo se strettamente indispensabile in relazione alle finalità di gestione, di manutenzione e/o di assistenza di volta in volta perseguita e, in ogni caso, limitatamente ai dati necessari per l'esecuzione dell'intervento richiesto. In conformità a quanto prescritto dal Garante nel sopraccitato Provvedimento generale, SANVIGO SRL informa che l'elenco aggiornato dei soggetti incaricati della funzione di amministratore di sistema, nei termini di cui si è detto, è conoscibile da ciascun dipendente/collaboratore mediante richiesta da inoltrare al Titolare.